IPA Software Engineering Center
Information-technology Promotion Agency, Japan

品質説明力の強化に向けた政府の取組みと業界の動向

独立行政法人　情報処理推進機構
技術本部ソフトウェア・エンジニアリング・センター
統合系プロジェクト＆組込み系プロジェクト　サブリーダー
工学博士　田丸喜一郎

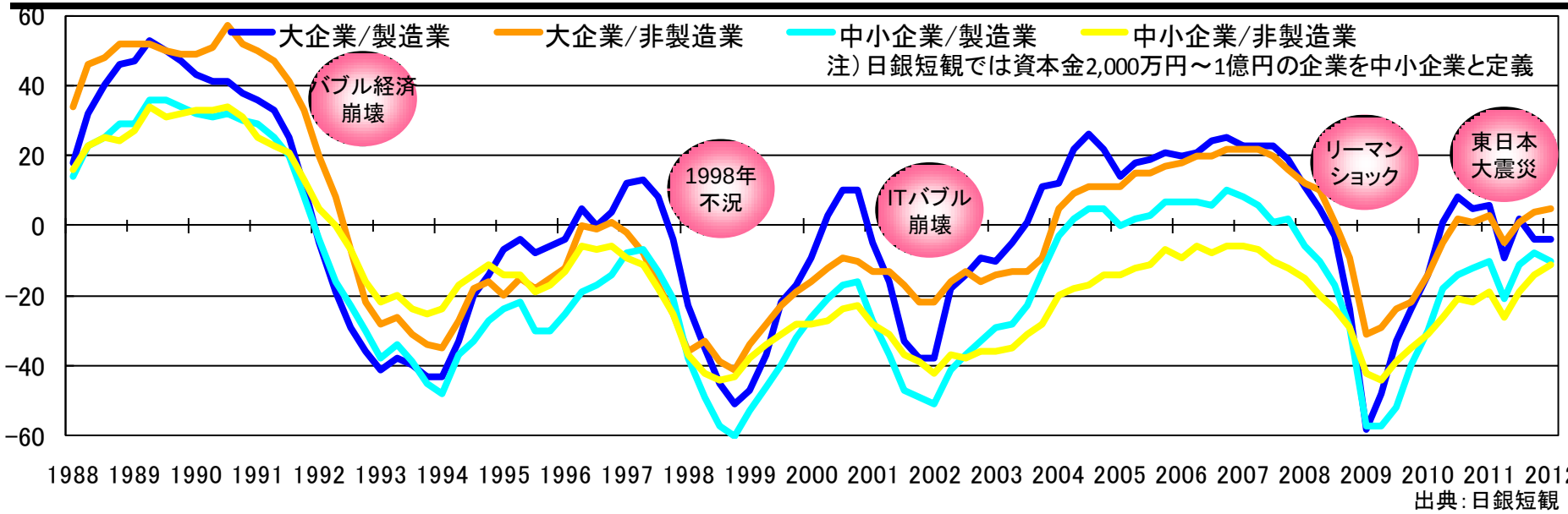
Copyright © 2012 IPA, All Rights Reserved

高度情報ネットワーク社会の登場

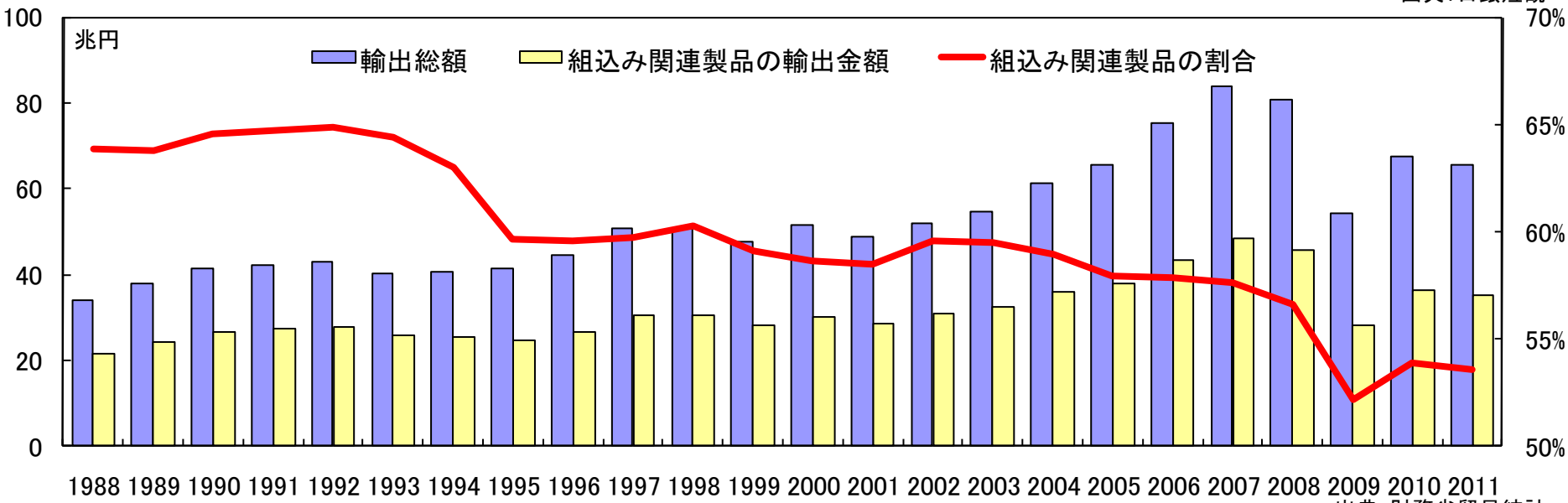
国民生活にとってITは水や空気のように「当たり前に」存在するもの

Copyright © 2012 IPA, All Rights Reserved

日銀短観(1988年3月～2012年3月:四半期毎)と輸出金額の推移(1988年～2011年暦年)



出典:日銀短観

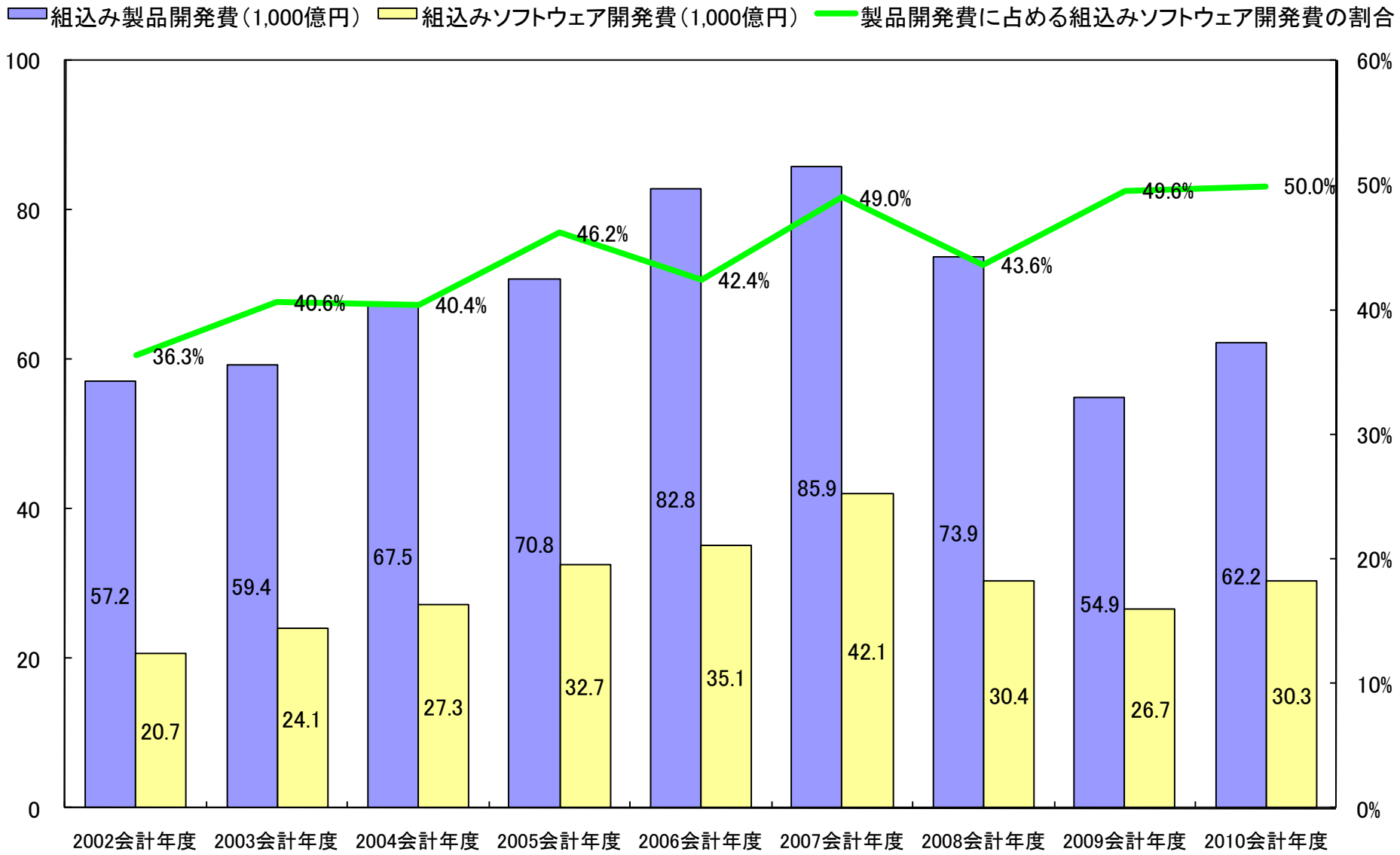


出典:財務省貿易統計

Copyright © 2012 IPA, All Rights Reserved

製品開発費と組込みソフトウェア開発費の推移

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri



出典：本調査、経済産業省「組込みシステム産業の実態把握調査」「組込みソフトウェア産業実態調査」、
一般社団法人 日本機械工業連合会（JMF）「機械工業生産額見通し調査」

Copyright © 2012 IPA, All Rights Reserved

新成長戦略が描くスマートコミュニティの将来像

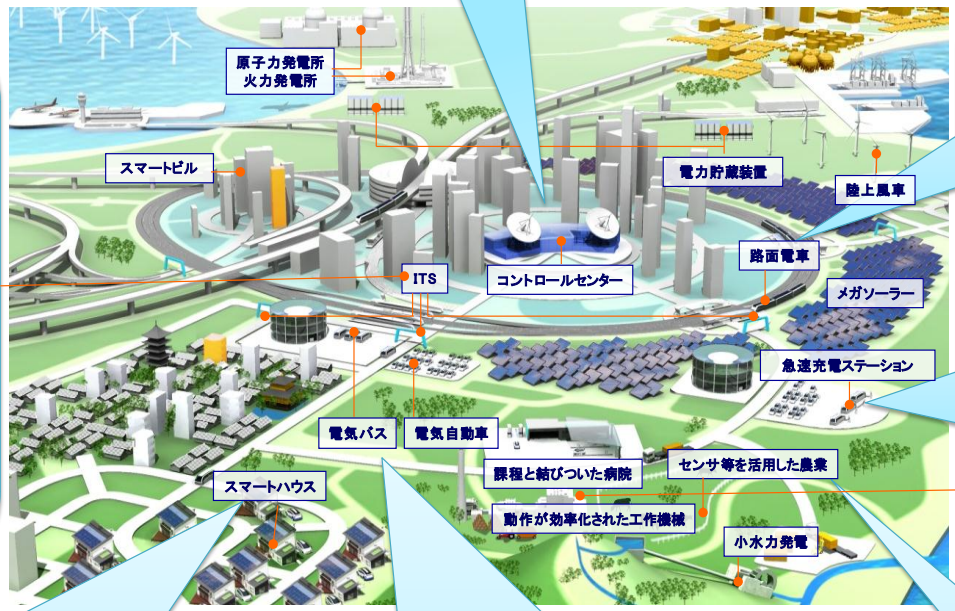
コントロールセンター

地域のエネルギー需給を最適化するコントロールセンター

- 太陽光発電、風力発電、小水力など自然エネルギーを電源として積極的に活用
- 変動の多い自然エネルギーを地域内で有効活用するため、各家庭やオフィスで余った電力を地域内で融通
- 電気バスや電気自動車の位置情報と充電状態を管理することで、これらの自動車を電力インフラとして活用

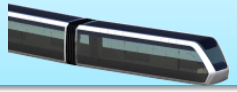
エネルギーネットワークと一体になった新しい交通インフラ

EVや電気バス同士で情報をやりとりすることにより、
飛躍的な低炭素化と事故や渋滞問題の解決を同時実現



架線レス路面電車

蓄電池を搭載した路面電車
駅での停車時：電池に充電
駅間の移動時：電池で駆動



急速充電ステーション

30分で80%充電

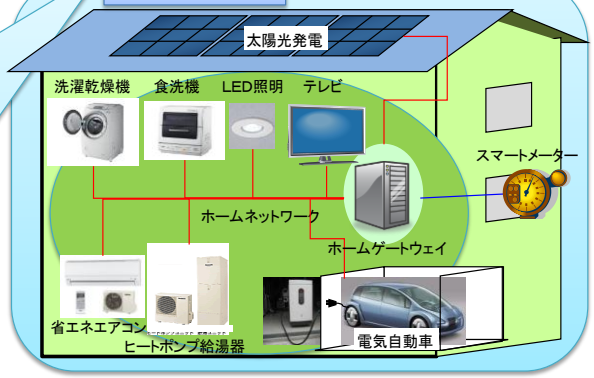
医療／ものづくりなど

・テーラーメード化された医療の提供
・GPSを活用した自動車両誘導システム

EVを電力インフラとして活用

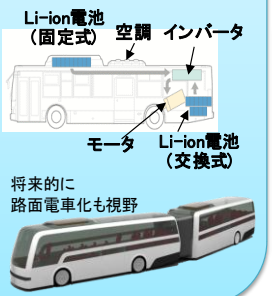
電力不足時：電気自動車→家庭
電力過剰時：家庭→電気自動車

スマートハウス



電気バス（将来は路面電車化）

電池交換式の電気バス。将来的には複数台を連結して路面電車化



センサ等を活用した農業

各種情報を分析し、
最適な生産手段を可能に

（出所）スマートコミュニティ関連システムフォーラム資料、三菱重工資料より経済産業省作成

Copyright © 2012 IPA, All Rights Reserved

基本的視座　～IT融合新産業の創出に向けて～

SEC
Software Engineering
for Mo･No･Zu･Ku･Ri

視座①

- 要素技術の強さのみでは勝てない時代に

視座②

- 「日本市場発」から「最初からグローバル」へ

視座③

- デジタル化・ネットワーク化によるIOC（Internet of Computers）からIOT（Internet of Things）へ

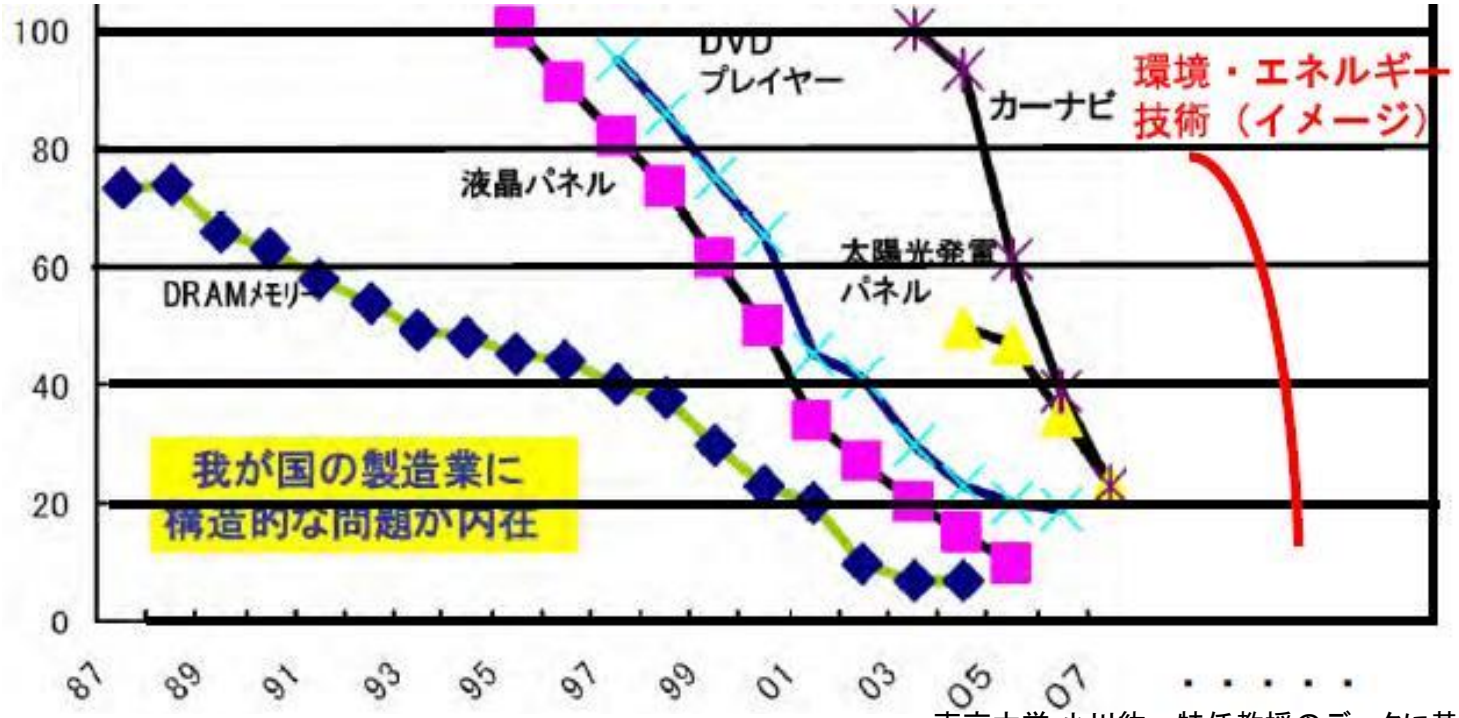
Copyright © 2012 IPA, All Rights Reserved

基本的視座①

『要素技術の強さのみでは勝てない時代に』

- 日本のIT・エレクトロニクス分野は「要素技術の宝庫」
- 他方、グローバル市場では、要素技術を駆使した日本製品は短期間でシェア下落

【日本製品の世界市場シェアの推移】



東京大学 小川紘一特任教授のデータに基づき経済産業省作成

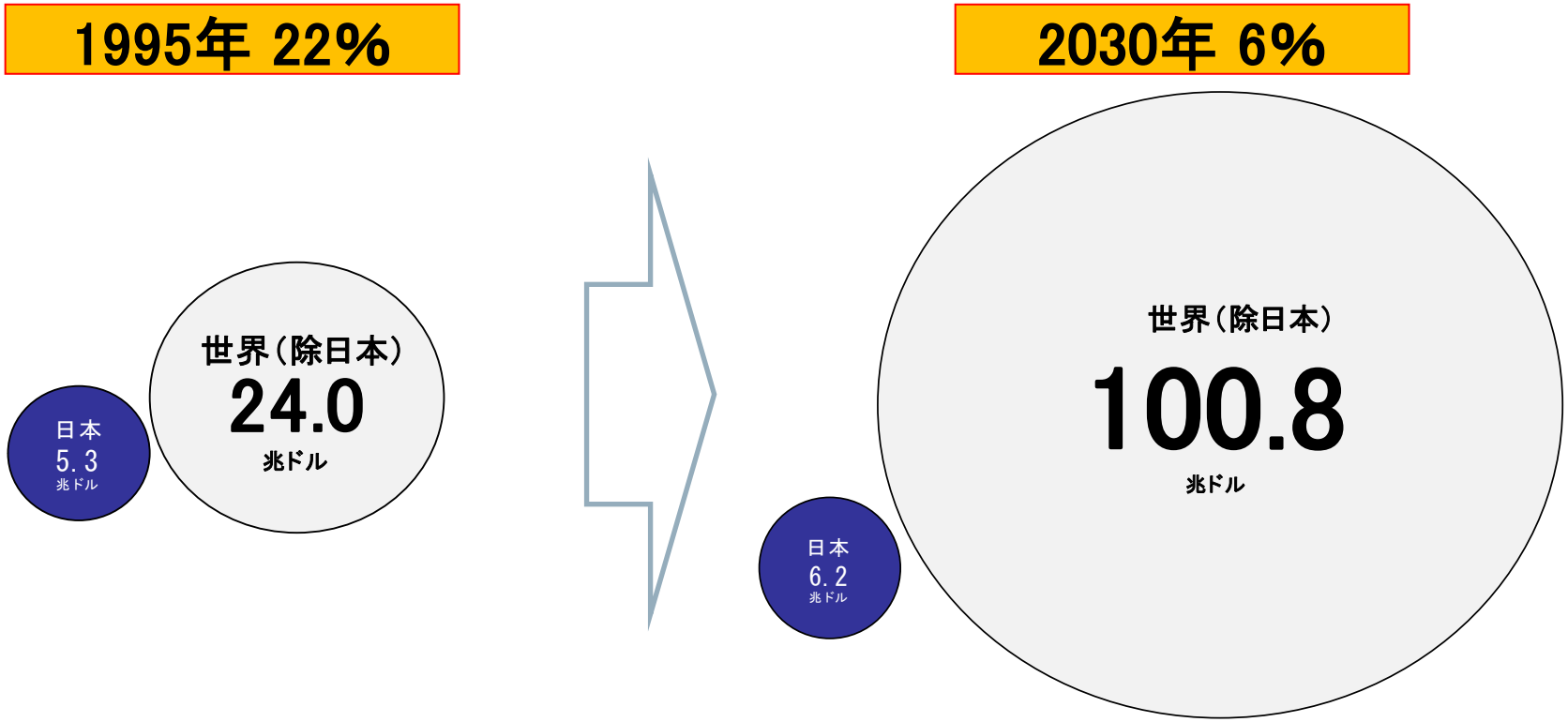
Copyright © 2012 IPA, All Rights Reserved

基本的視座②

『「日本市場発」から「最初からグローバル」へ』

- 2030年における日本市場は世界市場の約6%のみ
- 最初からグローバル市場を見据えた事業展開が重要

【世界と日本のGDP推移】



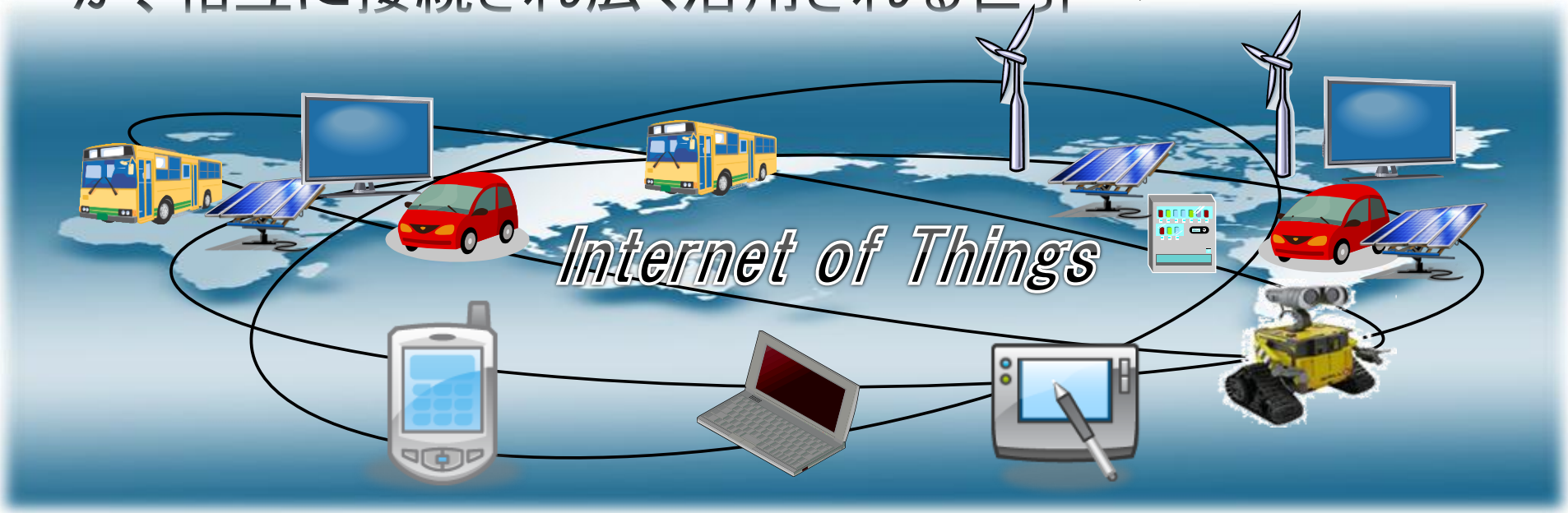
内閣府「世界経済の潮流」等より経済産業省作成

Copyright © 2012 IPA, All Rights Reserved

基本的視座③

『デジタル化・ネットワーク化によるIOC（Internet of Computers からIOT（Internet of Things）へ』

- 情報のデジタル化・ネットワーク化により、情報が、瞬時に、安価に、世界中で共有可能に
- あらゆるデジタル化された情報やネットワーク化された機器が、相互に接続され広く活用される世界へ



図出典：NTTデータ　ロボティクスインテグレーション推進室　取り組み説明資料

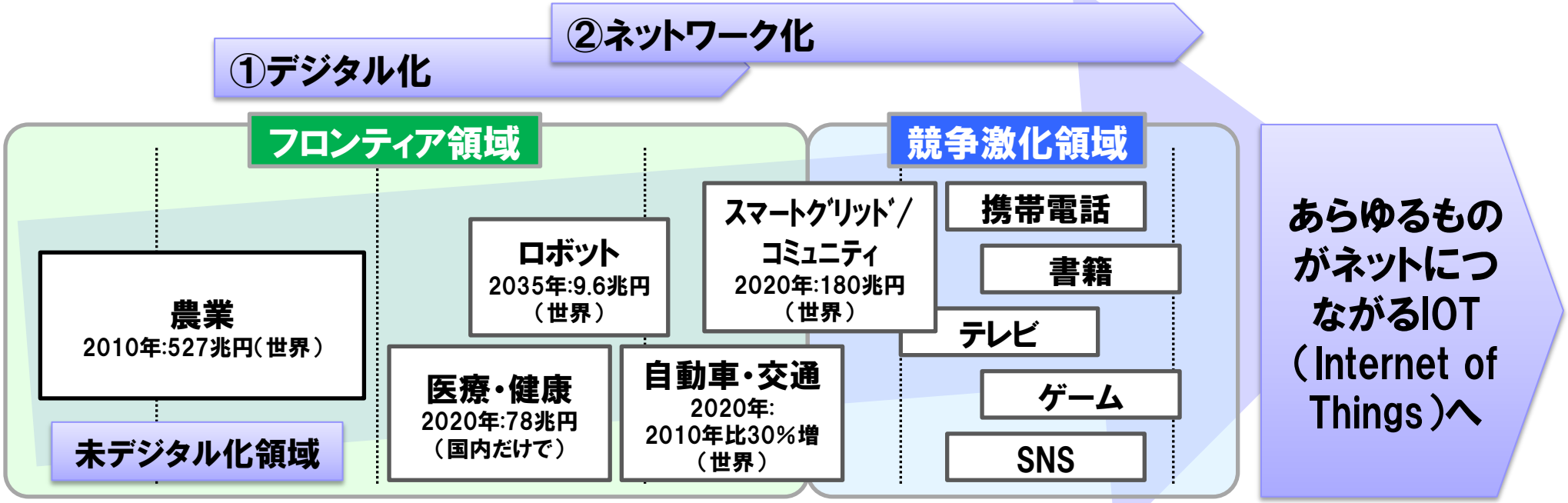
Copyright © 2012 IPA, All Rights Reserved

重点分野の考え方 （競争激化/フロンティア領域）

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

ITによる産業構造の変化と新規ビジネス創出の大きな機会が見込まれる領域に焦点

- 既に変化が始まっているスマートコミュニティ
- ネットワーク化の進展が今後見込まれる自動車、ロボット、医療
- 情報のデジタル化の進展が今後見込まれる農業等



出展：農業：韓国ロッテ社市場調査より抜粋、ロボット：経済産業省「ロボットの将来市場規模」(H22年4月)、自動車：みずほコーポレート銀行「次世代パワートレーン社の需要見通しとＥＶの展望」(H22年1月)、医療・健康：「新成長戦略」(H22年6月)、スマートコミュニティ：日経BP社「世界スマートシティ総覧」(H22年)

Copyright © 2012 IPA, All Rights Reserved

IT融合による新社会システムの創出に向けて

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

戦略重点分野に対する政策展開　＜理念から行動への移行＞

- ①融合システム産業フォーラム（仮称）
- ②IT融合システム設計・開発・輸出の支援
- ③事業化リスクマネー供給支援
- ④戦略的標準化活動の促進

政策による下支え

【重点6分野】

- スマートアグリシステム
- スマートヘルスケア産業
- 社会システムに組み込まれるロボット
- スマートコミュニティ
- 自動車と交通システム
- コンテンツ・クリエイティブビジネス

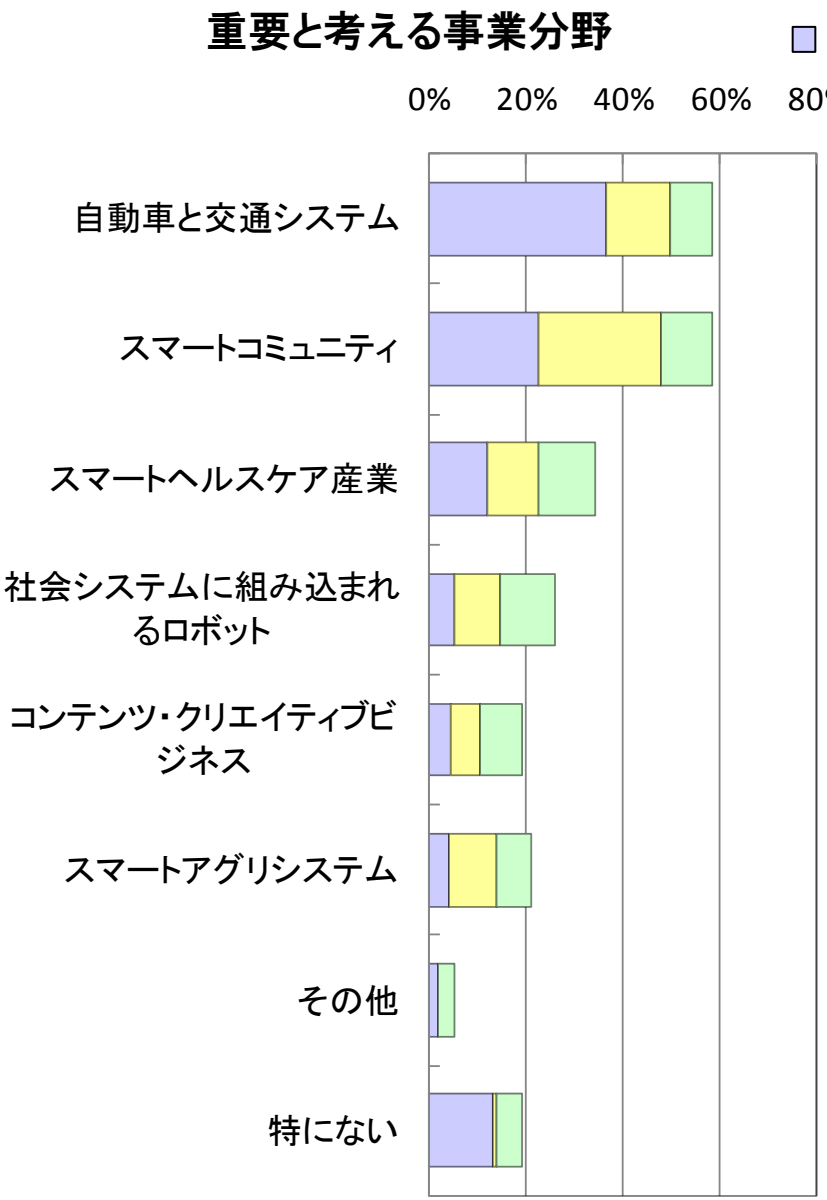
横断的課題解決

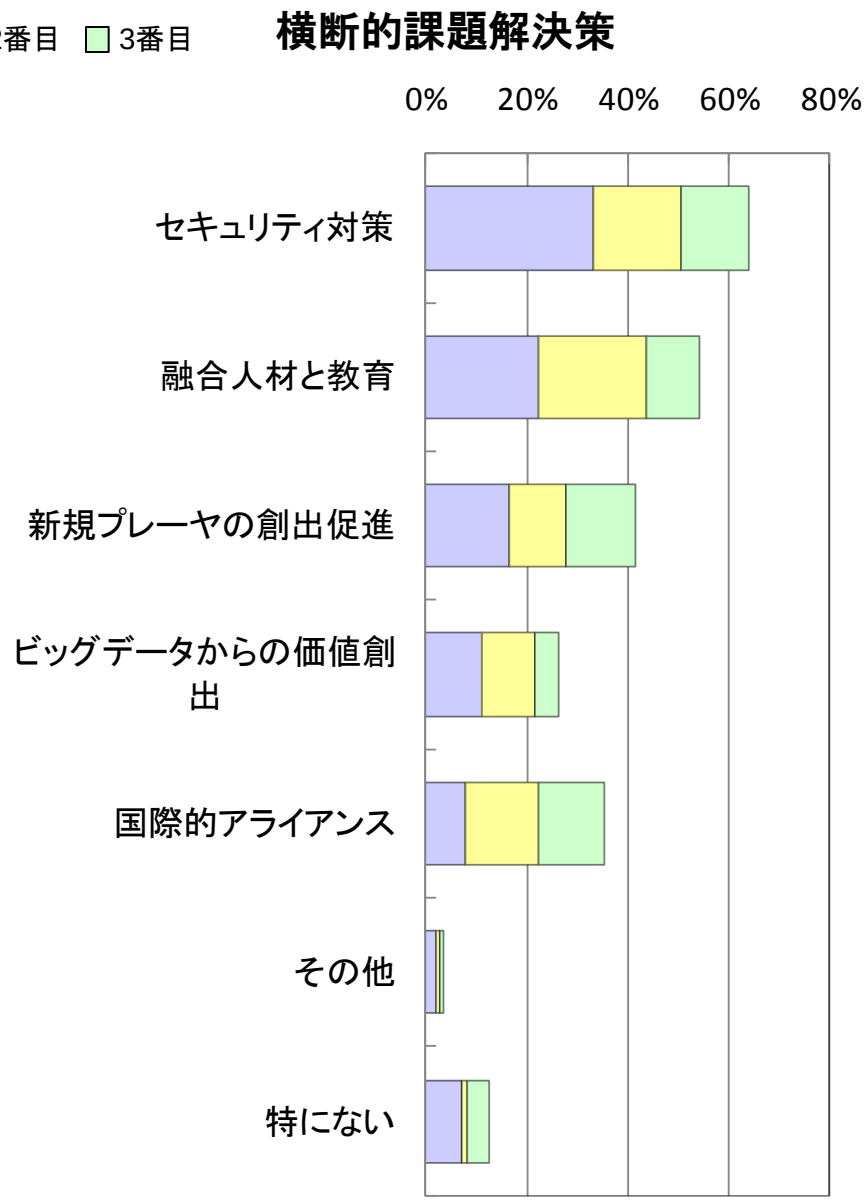
- セキュリティ対策
- IT融合人材と教育
- ビッグデータからの価値創出
- 国際的アライアンス
- 新規プレーヤ創出促進

【横断的課題】

経済産業省の戦略重点6分野で重要と考える事業分野と横断的課題解決策

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri



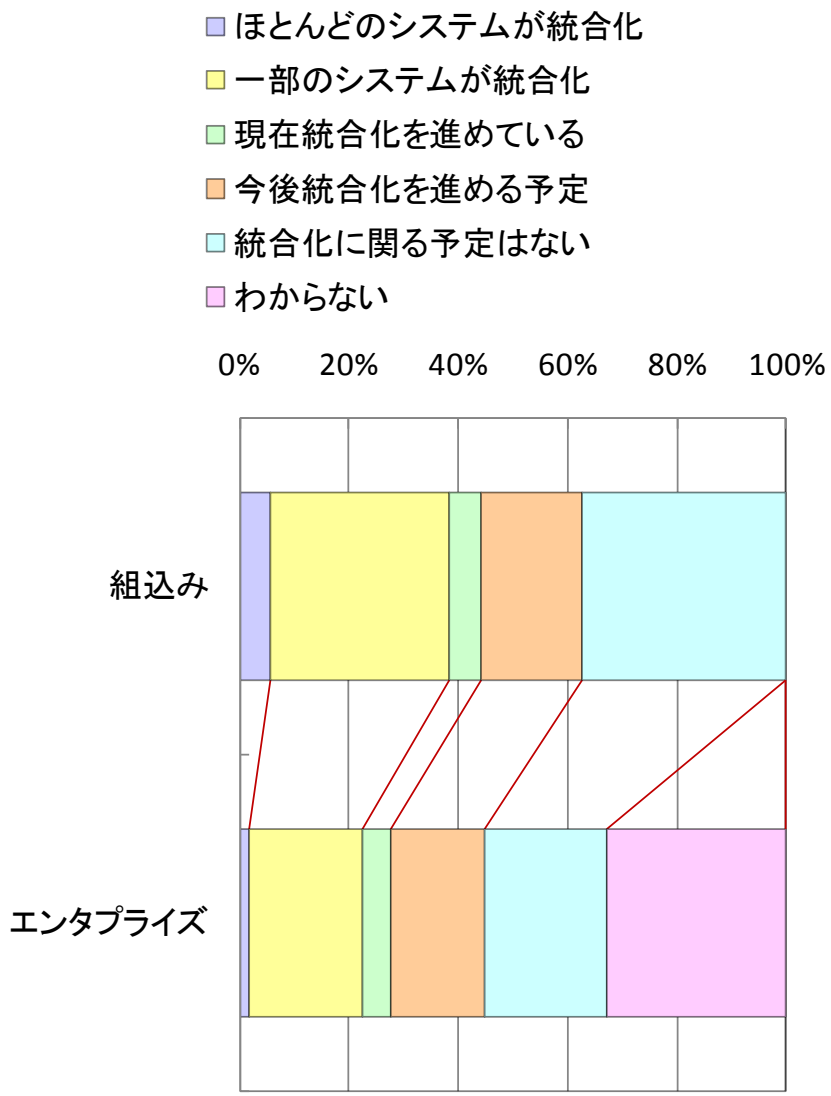


Copyright © 2012 IPA, All Rights Reserved

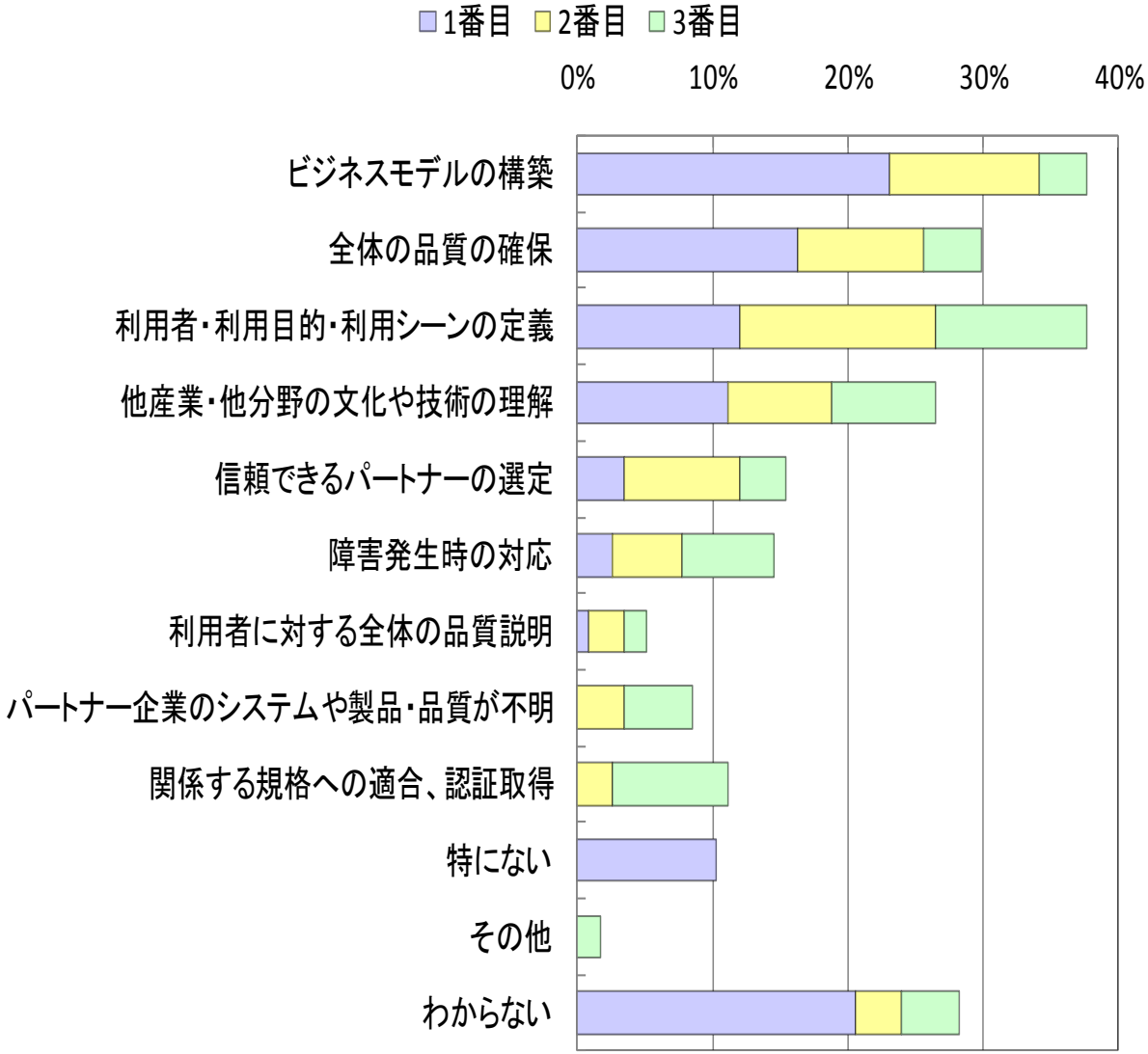
統合システム関連の対応状況と課題認識

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

統合システム関連の対応状況



統合システム実現の課題(組込み)

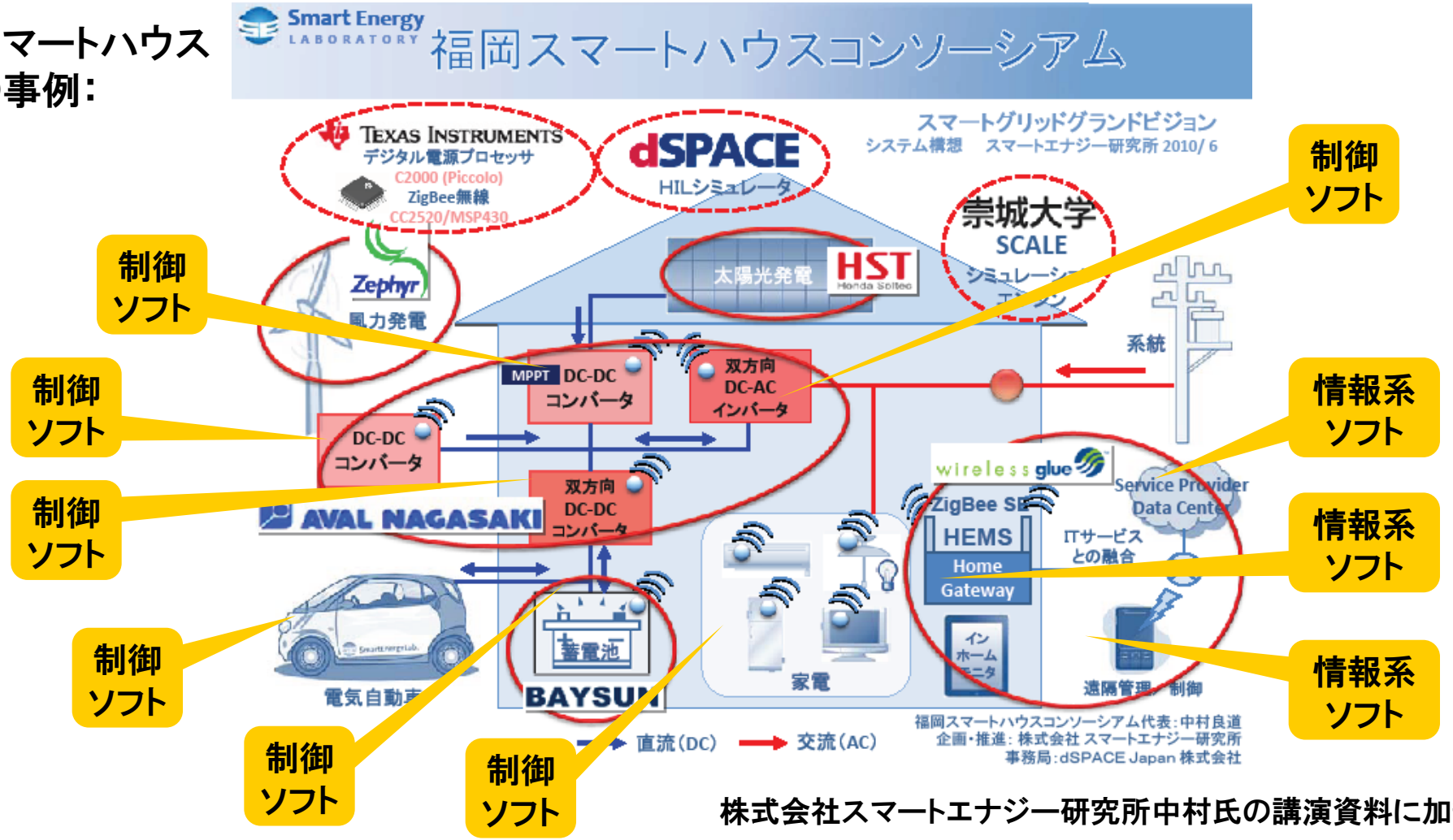


Copyright © 2012 IPA, All Rights Reserved

統合システムとしてのスマートハウス

スマートハウスの電源制御システムは**複数の装置メーカ**から提供される**ソフトウェア制御**のサブシステムから構成される**統合システム** ⇒ 全体システムとしての信頼性の確保は？

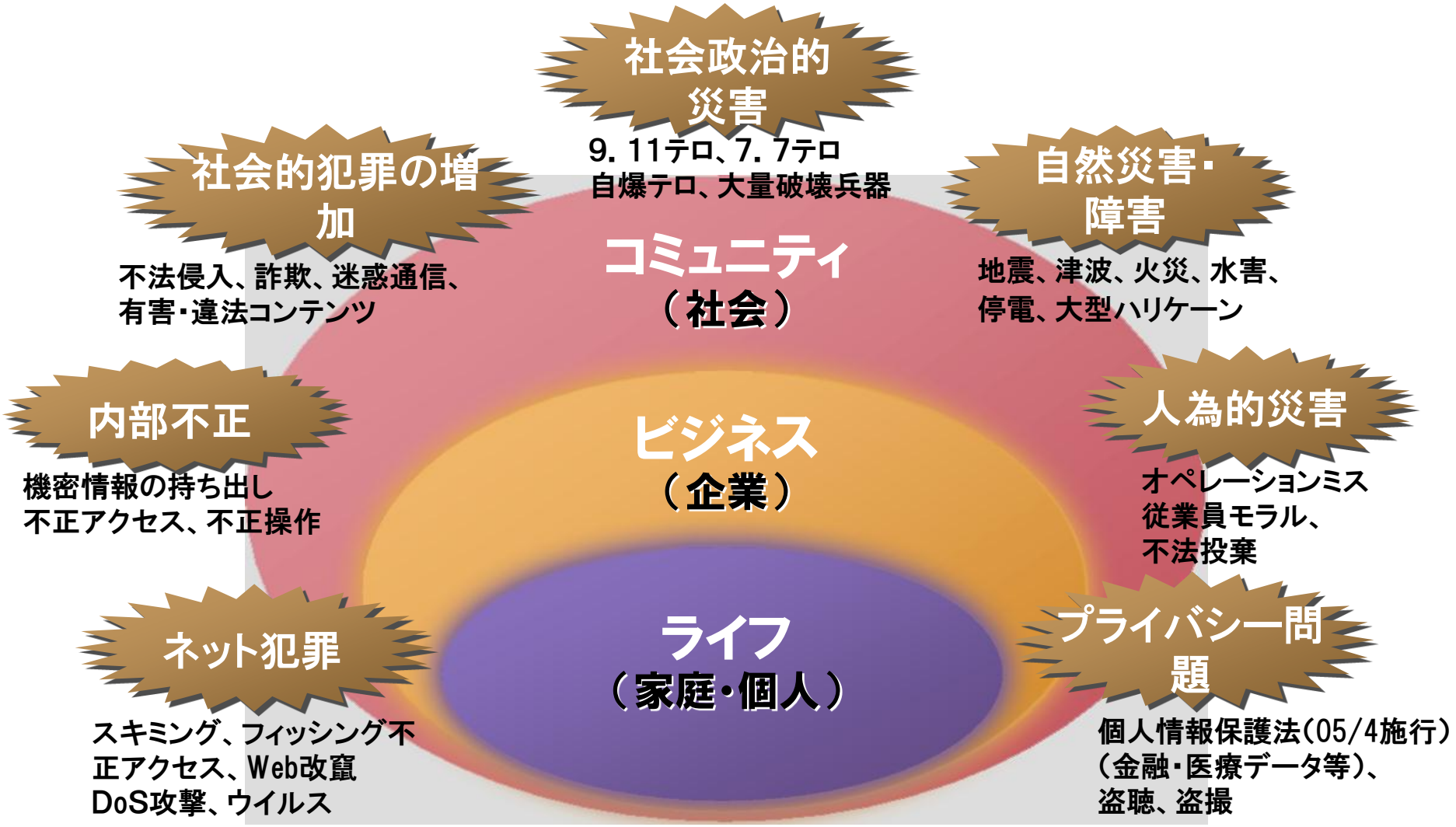
スマートハウスの事例：



株式会社スマートエナジー研究所中村氏の講演資料に加筆

Copyright © 2012 IPA, All Rights Reserved

多様化するセキュリティ脅威



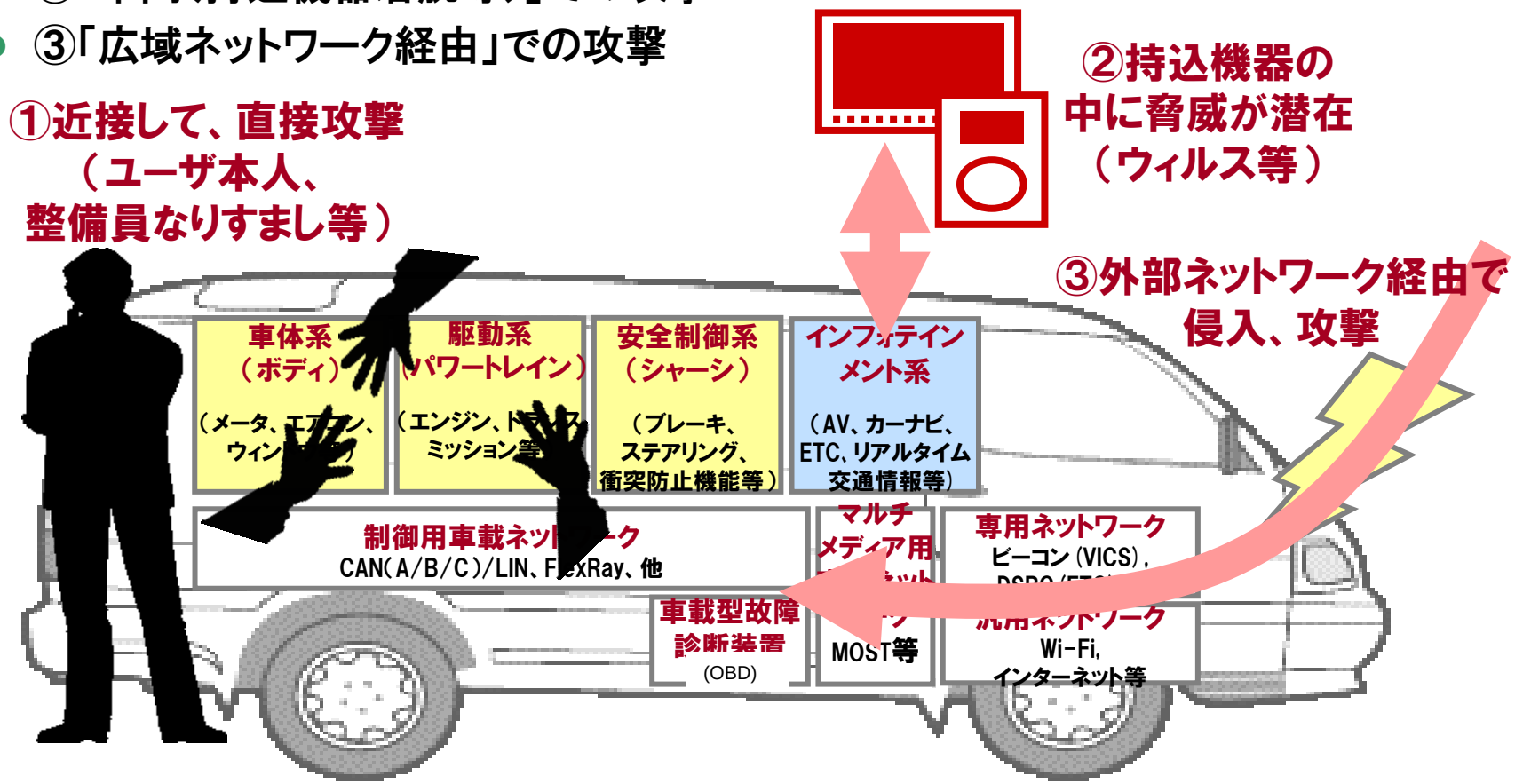
「不安解消」、「安心・安全の確保」に対する社会的ニーズ増大

Copyright © 2012 IPA, All Rights Reserved

自動車に対するセキュリティ脅威

自動車本体に対する攻撃の3パターン

- ①「近接」での攻撃
- ②「中間（持込機器着脱等）」での攻撃
- ③「広域ネットワーク経由」での攻撃

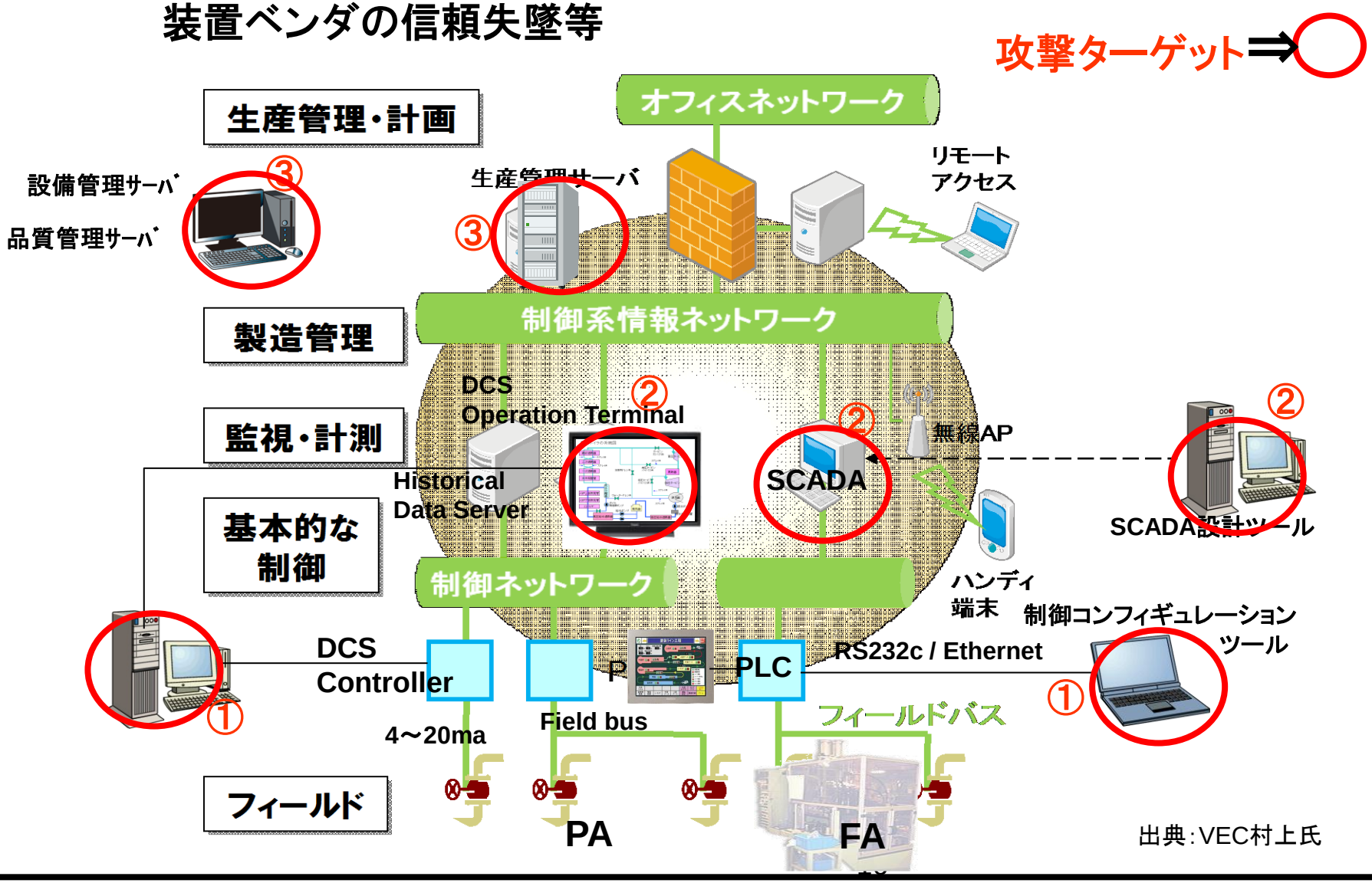


スマートフォンの普及によって、より自動車と情報システムの連携が強化される。
より便利な自動車社会を構築するには、情報セキュリティへの考慮は必須。

Copyright © 2012 IPA, All Rights Reserved

制御システムに対するセキュリティ脅威

攻撃目的:装置や設備の破壊、悪品質製品生産や生産の暴走、装置ベンダの信頼失墜等



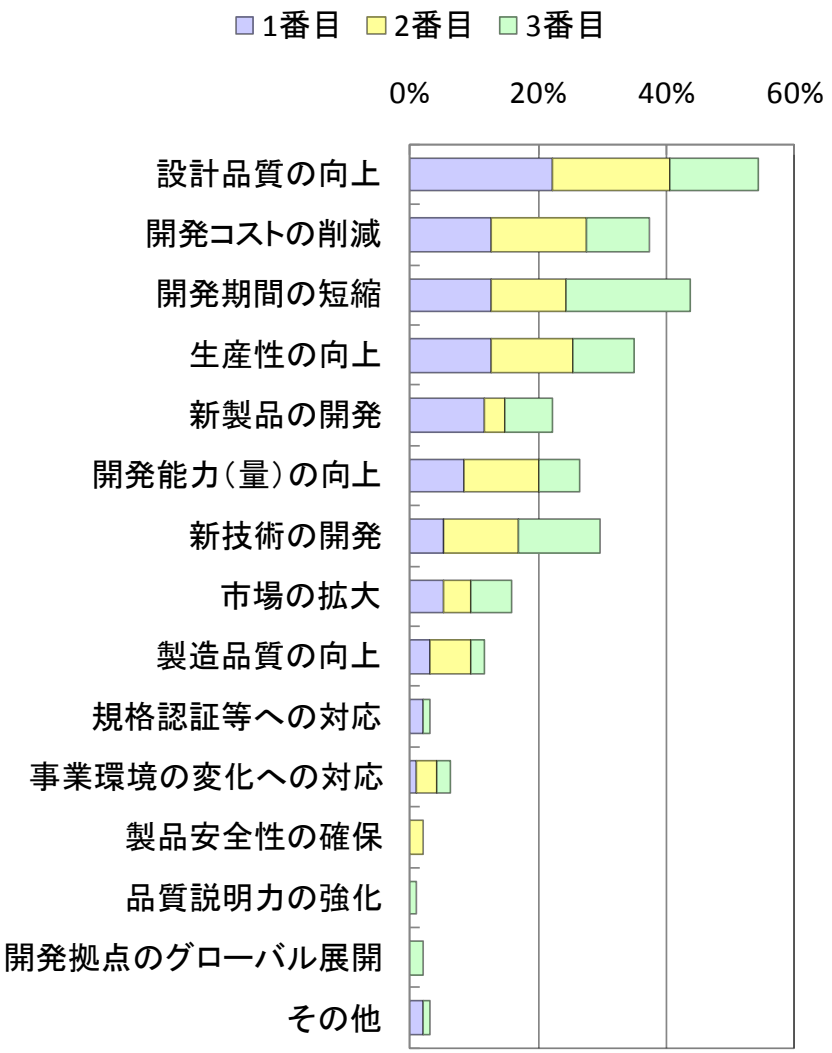
出典:VEC村上氏

Copyright © 2012 IPA, All Rights Reserved

組込みソフトウェア開発の課題

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

2012年　組込みソフトウェア開発の課題



1番目の課題Top10の推移（2007～2012）

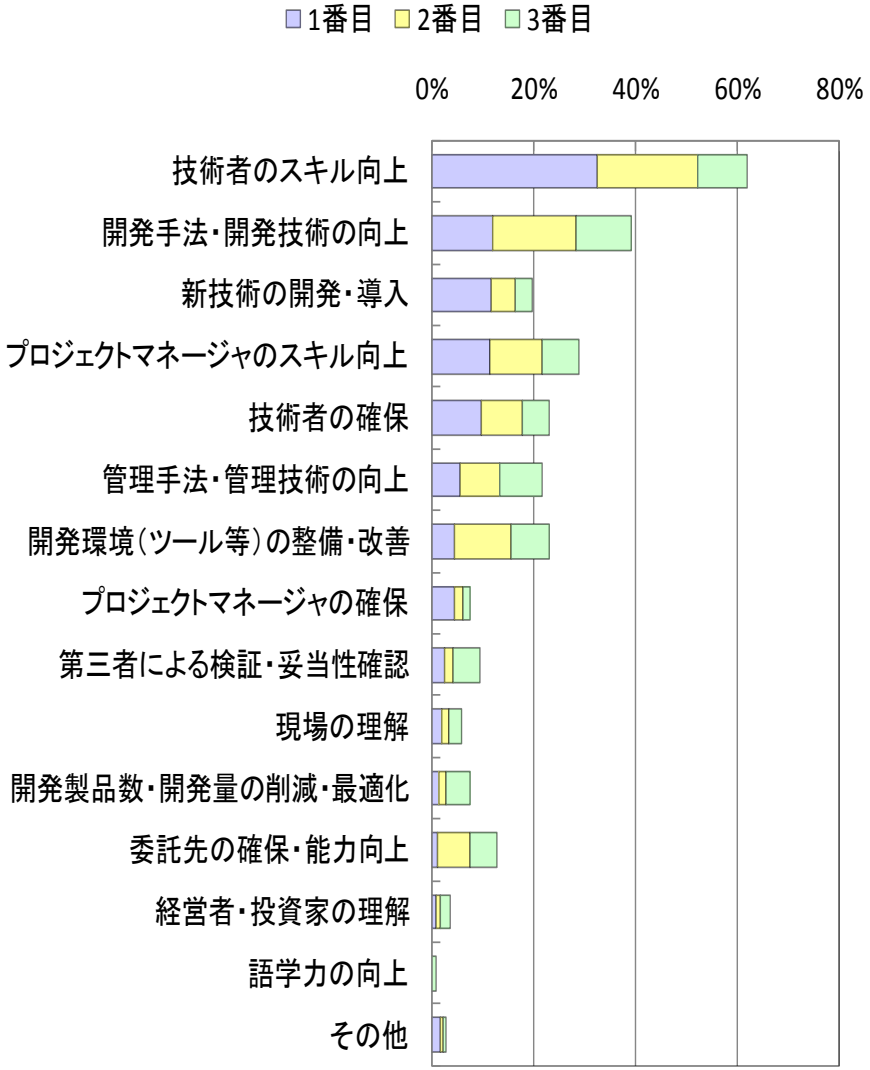
2007	2008	2009	2010	2011	2012
設計品質	設計品質	設計品質	設計品質	設計品質	設計品質
新製品	新製品	開発期間	開発コスト	新製品	開発コスト
開発期間	開発期間	生産性	新技術	開発コスト	開発期間
開発能力	開発能力	開発コスト	新製品	市場拡大	生産性
生産性	開発コスト	開発能力	市場拡大	開発能力	新製品
開発コスト	生産性	新技術	開発能力	新技術	開発能力
市場拡大	市場拡大	製造品質	開発期間	開発期間	新技術
新技術	新技術	新製品	製品安全	生産性	市場拡大
製品安全	製品安全	市場拡大	生産性	製造品質	製造品質
製造品質	製造品質	製品安全	製造品質	事業環境変化対応	規格認証

Copyright © 2012 IPA, All Rights Reserved

組込みソフトウェア開発課題に有効な解決策

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

2012年　各課題解決の有効な解決策の合計



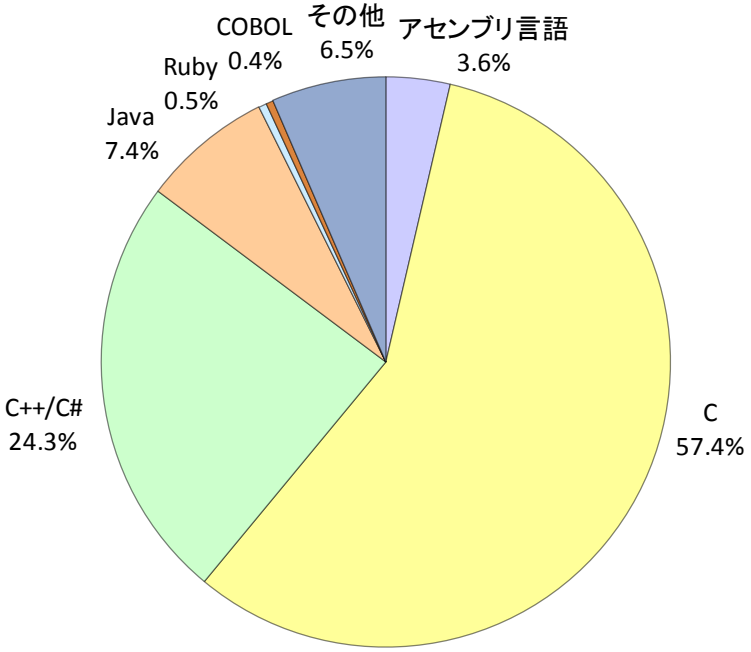
1番目の解決策Top10の推移（2007～2012）

2007	2008	2009	2010	2011	2012
技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上	技術者スキル向上
技術者の確保	技術者の確保	PMのスキル向上	PMのスキル向上	開発技術の向上	開発技術の向上
PMのスキル向上	PMのスキル向上	開発技術の向上	開発技術の向上	PMのスキル向上	新技術開発・導入
開発技術の向上	開発技術の向上	PMの確保	技術者の確保	技術者の確保	PMのスキル向上
PMの確保	PMの確保	技術者の確保	新技術開発・導入	新技術開発・導入	技術者の確保
管理技術の向上	管理技術の向上	管理技術の向上	PMの確保	PMの確保	管理技術の向上
新技術開発・導入	新技術開発・導入	新技術開発・導入	管理技術の向上	管理技術の向上	開発環境の整備
開発環境の整備	開発環境の整備	開発製品数最適化	委託先の確保	委託先の確保	PMの確保
開発製品数最適化	委託先の確保	開発環境の整備	開発環境の整備	開発製品数最適化	第三者による検証
経営者の理解	経営者の理解	委託先の確保	経営者の理解	経営者の理解	現場の理解

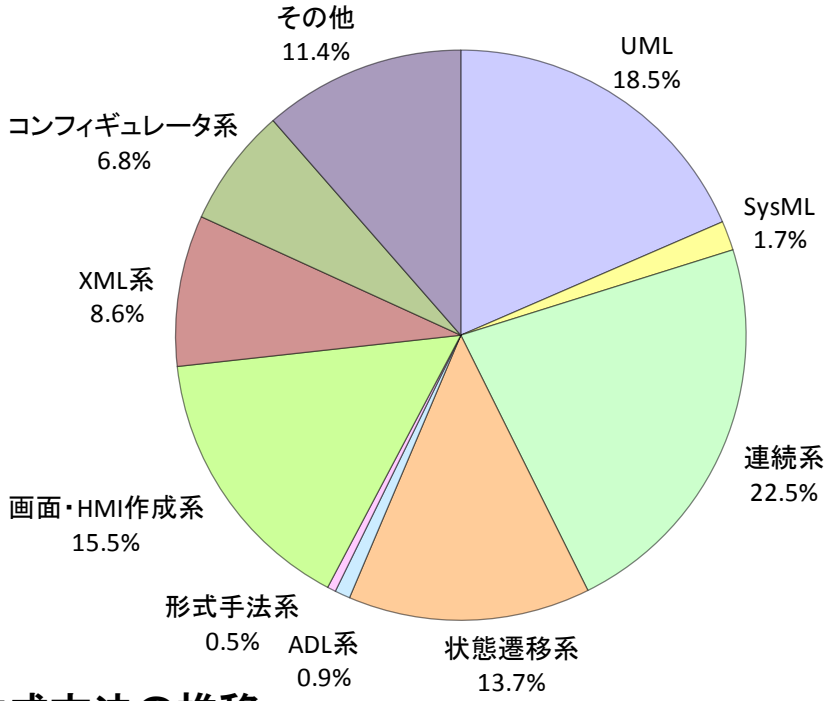
Copyright © 2012 IPA, All Rights Reserved

使用しているプログラミング言語

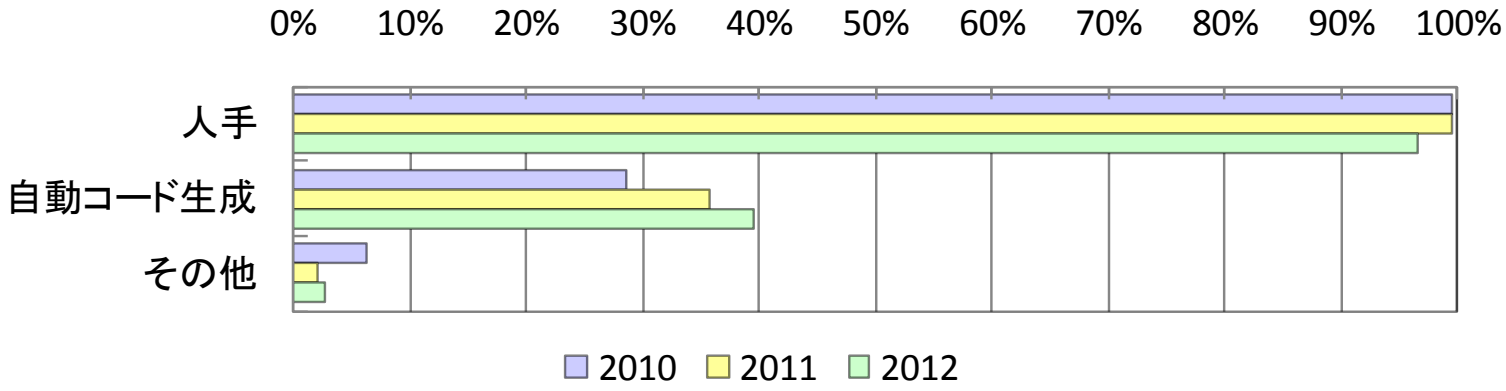
使用しているプログラミング言語（人手）



使用しているモデルベース言語（自動コード生成）

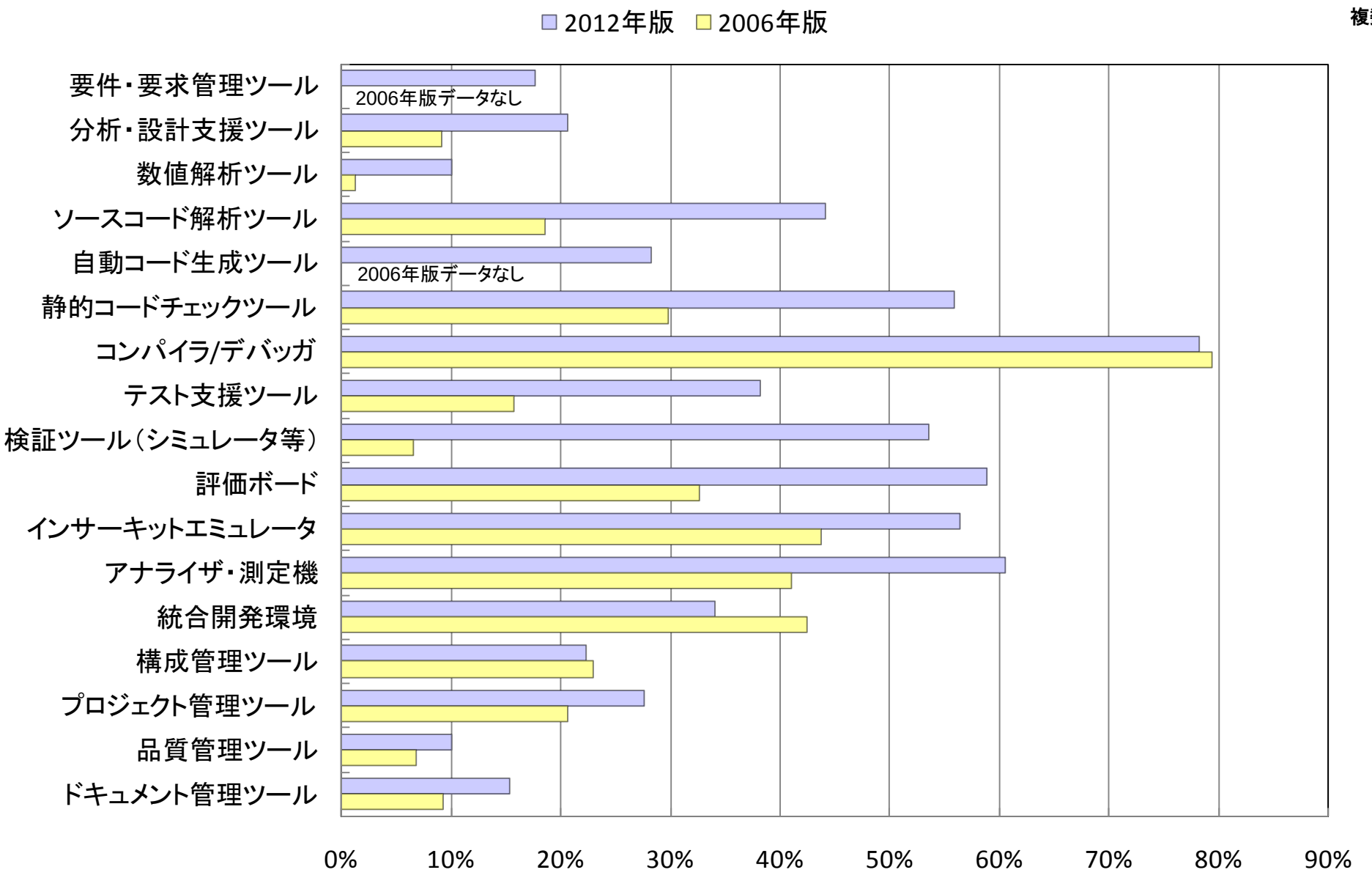


プログラムコード作成方法の推移



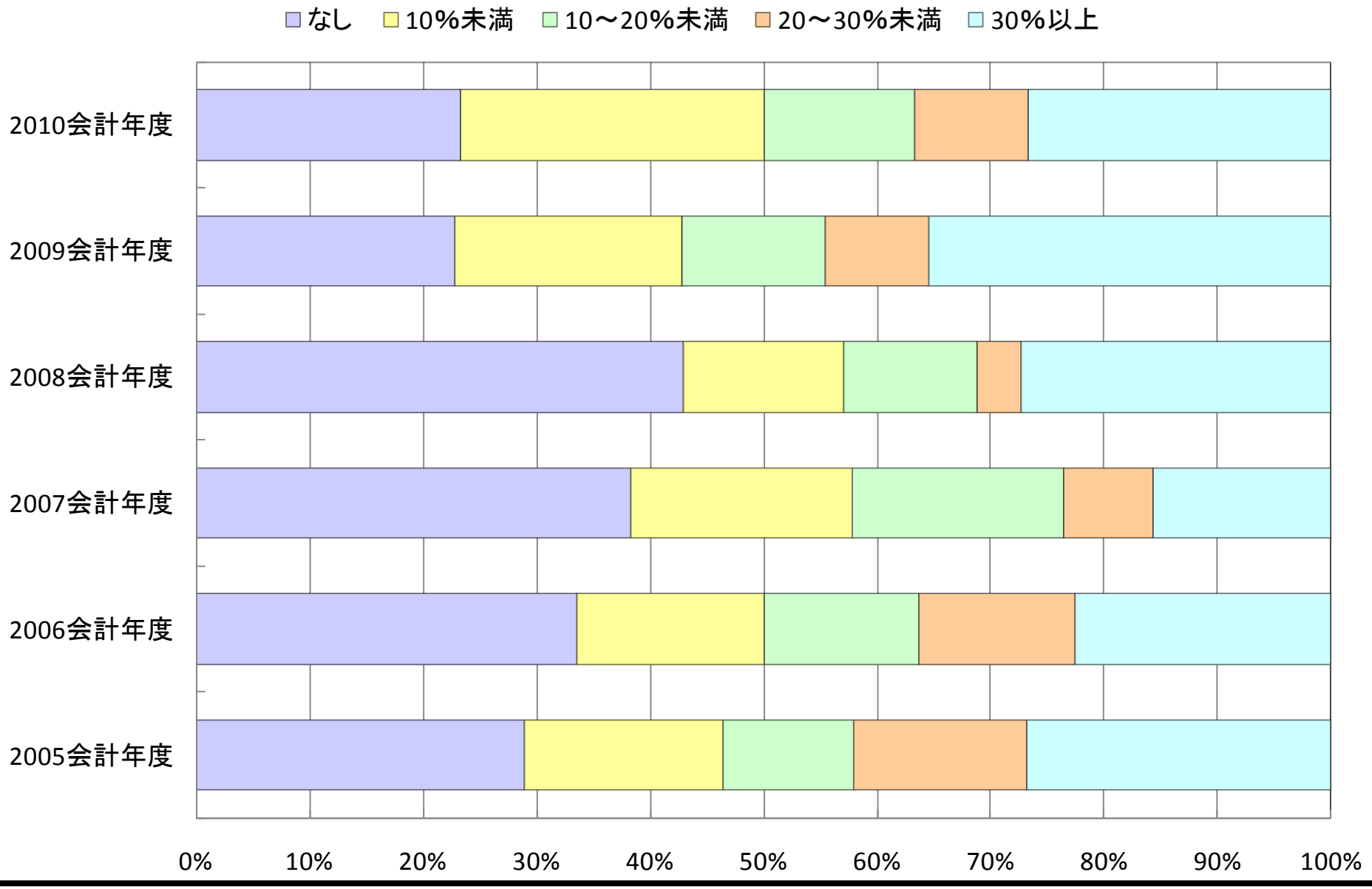
Copyright © 2012 IPA, All Rights Reserved

ツールの利用状況(経済産業省2006年版との比較)



Copyright © 2012 IPA, All Rights Reserved

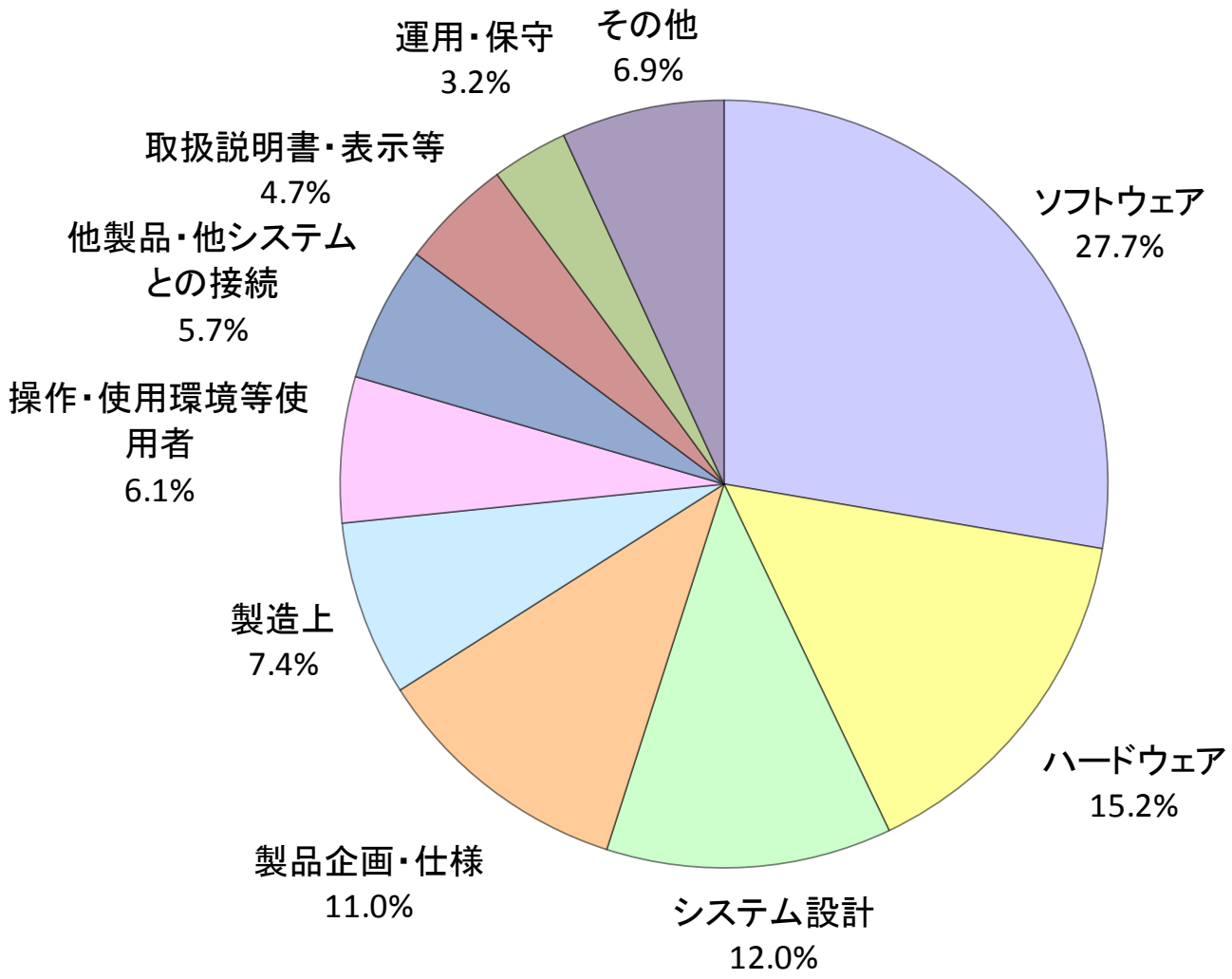
製品出荷後の不具合発生製品率の推移



Copyright © 2012 IPA, All Rights Reserved

製品出荷後に発生した不具合の原因

不具合の原因（製品数ベース）



Copyright © 2012 IPA, All Rights Reserved

ご参考：消費者事故等の調査機関の設置

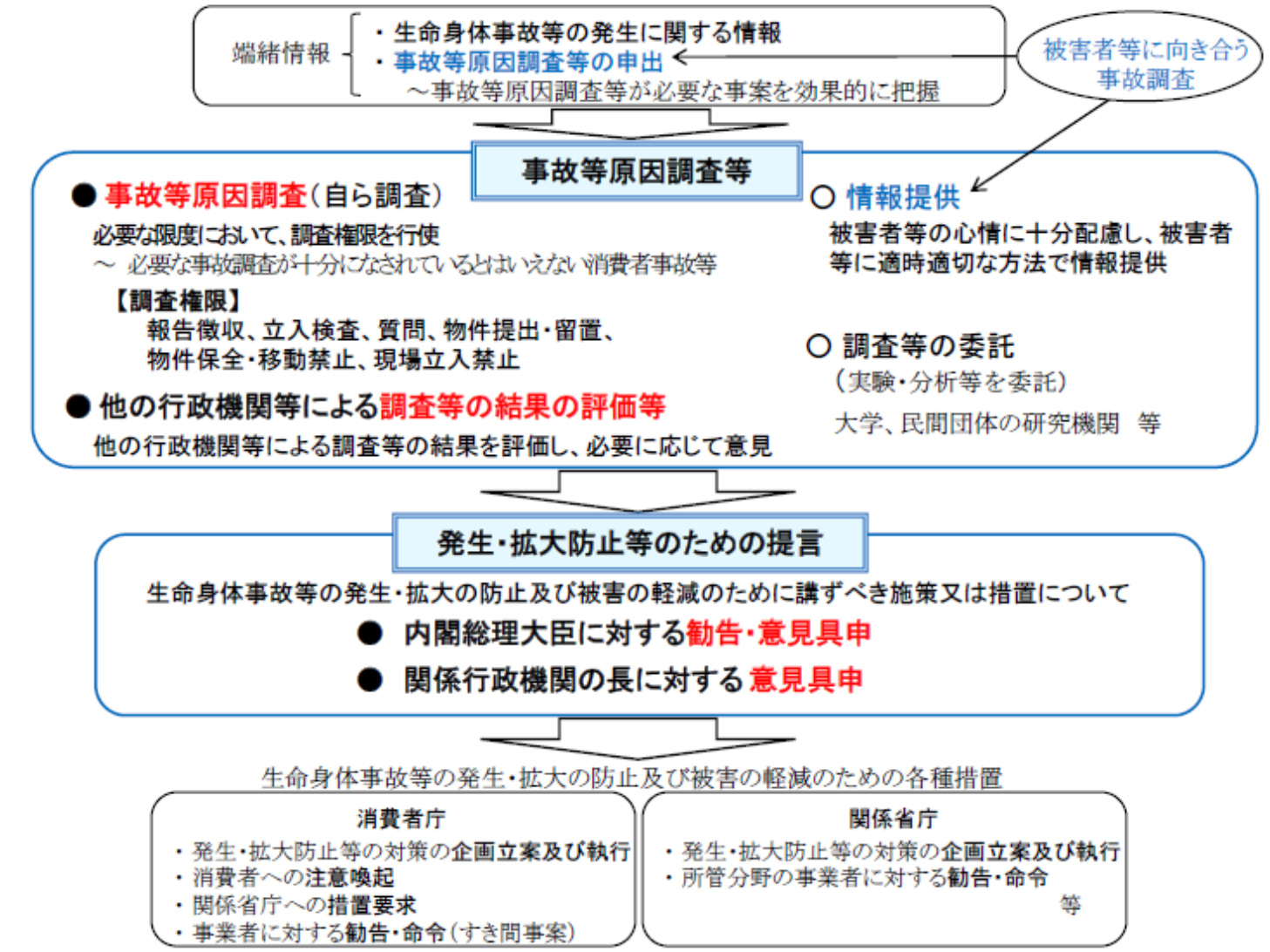
消費者安全法の一部を改正する法律（平成24年10月1日より施行）

消費者安全調査委員会（仮称）の設置

【 組 織 】
○委員（7名・非常勤）
（合議制の機関、委員は独立して職権を行使）
○臨時委員、専門委員
（必要に応じて任命）

【調査対象】
○生命・身体分野の消費者事故等　製品・食品・施設・役務を広く対象（運輸安全委員会の調査対象とされている事故等を除く）
○生命身体事故等の発生・拡大の　防止及び被害の軽減を図るために原因究明する必要性が高いもの

【事故等原因調査等、提言のイメージ】



出典：消費者庁ホームページ　http://www.caa.go.jp/soshiki/houan/pdf/120214_1-2.pdf

Copyright © 2012 IPA, All Rights Reserved

安全・安心なIT社会の実現に向けた2つの視点

1. 高い品質のソフトウェアを作ること

- 仕様通りソフトウェアを正しく作る
- 用途に適合した正しいソフトウェアを作る

→ ソフトウェア開発力の強化

2. 高い品質を客観的に説明できること

→ ソフトウェア品質説明力の強化

Copyright © 2012 IPA, All Rights Reserved

第三者の検証・妥当性確認による品質説明力強化

SEC
Software Engineering
for Mo・No・Zu・Ku・Ri

品質説明に対する市場意識の変化

品質説明力の不足： 当事者企業の技術的主張だけでなく、第三者の裏付け（検証、妥当性確認）による品質説明への要求の増大

製品の利用者とのギャップの拡大

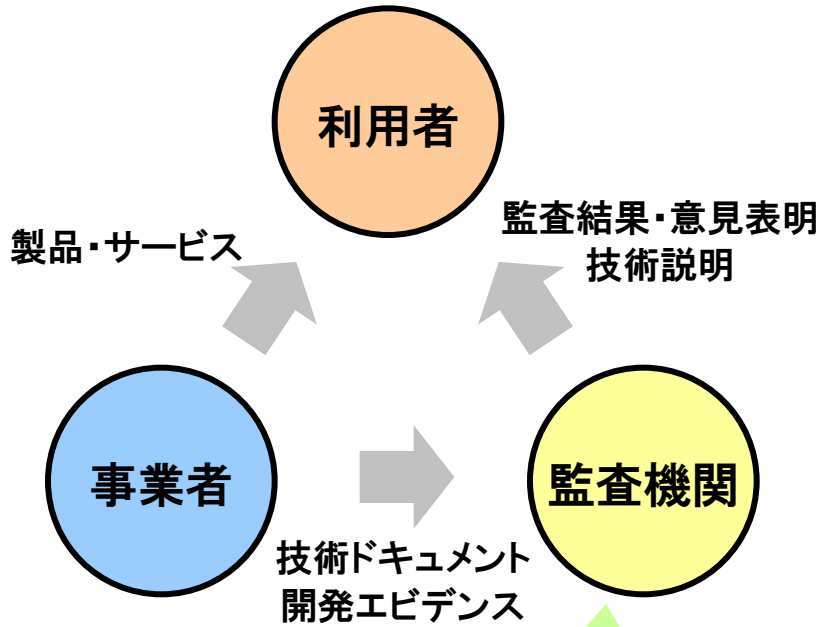
利用品質低下の懸念： 製品・システムの高度化・複雑化と利用者の多様化により、製品・システムと利用者との間のギャップが拡大

先端技術製品の潜在リスクへの不安

製品品質低下の懸念： 技術の急速な進歩により技術標準（規格）に基づく規格認証の対象範囲外となる領域が拡大

品質文化の異なる業界を跨るシステム

残存する潜在リスクの増加： 複数の業界を跨るシステムの拡大に伴い、全体システムとしての品質確認の精度が低下



第三者による検証・妥当性確認

事業者の技術的主張の妥当性を、監査機関が開発技術水準と利用技術水準を考慮して第三者の立場で評価し、技術に関する専門知識のない利用者にも理解できる形で情報提供する仕組み

（会計処理における会計監査と同等の役割）

IPA/SECでの活動経緯

- 2010年3月：産構審情報システム・ソフトウェア小委員会にて第三者による検証・妥当性確認の枠組みの必要性が示される
- 2010年4月：IPA/SECの統合系プロジェクト内に検討チームを発足
- 2010年7月：調査活動開始
- 2010年11月：制度検討委員会発足（主査：名古屋大学高田教授）
- 2011年9月：第一次中間報告公開
- 2012年11月：部会活動報告書公開

Copyright © 2012 IPA, All Rights Reserved

ソフトウェア品質説明力強化の狙いと効果

国民生活の安全・安心・快適の向上と我が国産業の国際競争力の強化

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

ソフトウェア品質説明力強化の狙い	ソフトウェア品質説明力強化の効果
企業の製品・システムに関する利用者や市場への分かり易い品質説明	技術の専門家ではない利用者の安心感の向上
国際市場における日本製品・システムの品質に対する正当な評価の確立	我が国産業の国際競争力の維持・強化
産業界の枠を超えた品質の見える化による複数の産業界を跨り構成される高度なシステムの開発加速（例：スマートコミュニティシステムなど）	国民生活の快適性・利便性の向上 新成長戦略分野における我が国産業の国際優位性の確保
製品・システムの本質的な品質向上	国民生活の安全性の確保

ご参考：米国の状況

- 2010年日本製自動車の制御システムに対する不具合の疑念が拡大。米国政府の要請で、NASAの独立検証・妥当性確認(IV&V)センターが第三者の立場で、制御システムの検証ならびに妥当性確認を実施。2011年2月、不具合が発見されなかったとの最終報告が公開。
- 当事者企業の主張だけでなく、第三者の主張がないと説明力が不充分との意識（会計処理における会計監査の必要性と同等の意識）。
- 国防省やNASAのシステムの調達、航空機分野、医療機器分野で類似した仕組みを運用している。

Copyright © 2012 IPA, All Rights Reserved

ソフトウェア品質説明力強化のためのフレームワーク

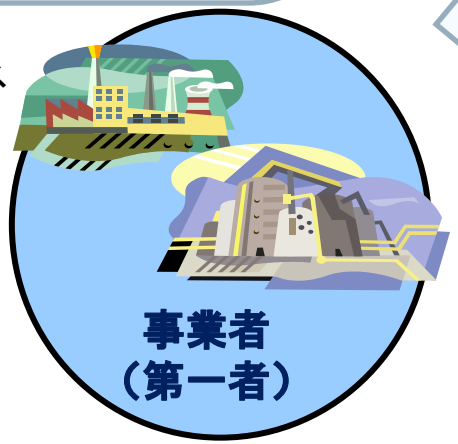
SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

【国民生活の安全・安心】
第三者である監査機関の意見も参考に製品・サービスを安心して利用できる

【事業者の主張】
この製品・サービスは一定の条件下において安全に使えます。

- 製品・サービスの安全、安心に係る品質目標
- 品質目標を達成するために必要な手段
- 手段を実施した証拠
- 品質目標、手段、証拠のトレーサビリティ

基本的にはセーフティケース、アシュアランスケースと同一の考え方に基づいている。



監査対象：
ソフトウェアが重要な役割を担う製品・サービス
（例：スマートコミュニティ、自動車など）

記述書

監査結果

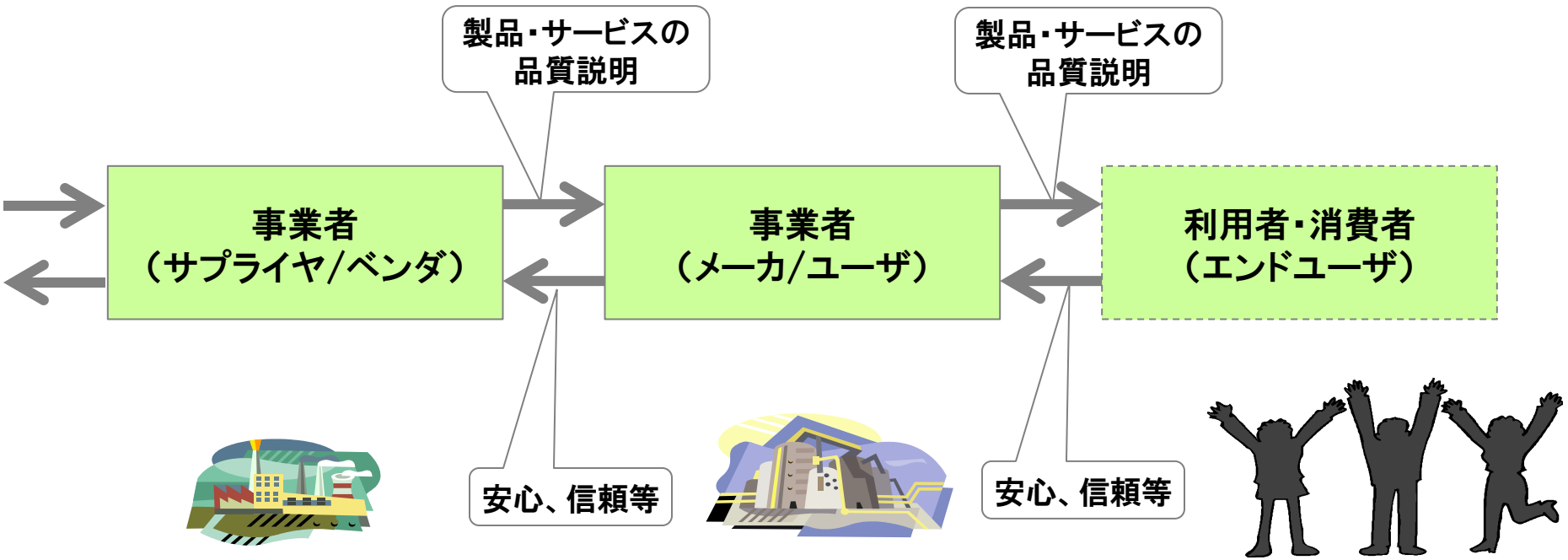
【監査機関の意見】
事業者の主張は適正です。

設計書など

【監査のための証拠】
製品・サービスのテスト結果、設計書、開発手順などの証拠

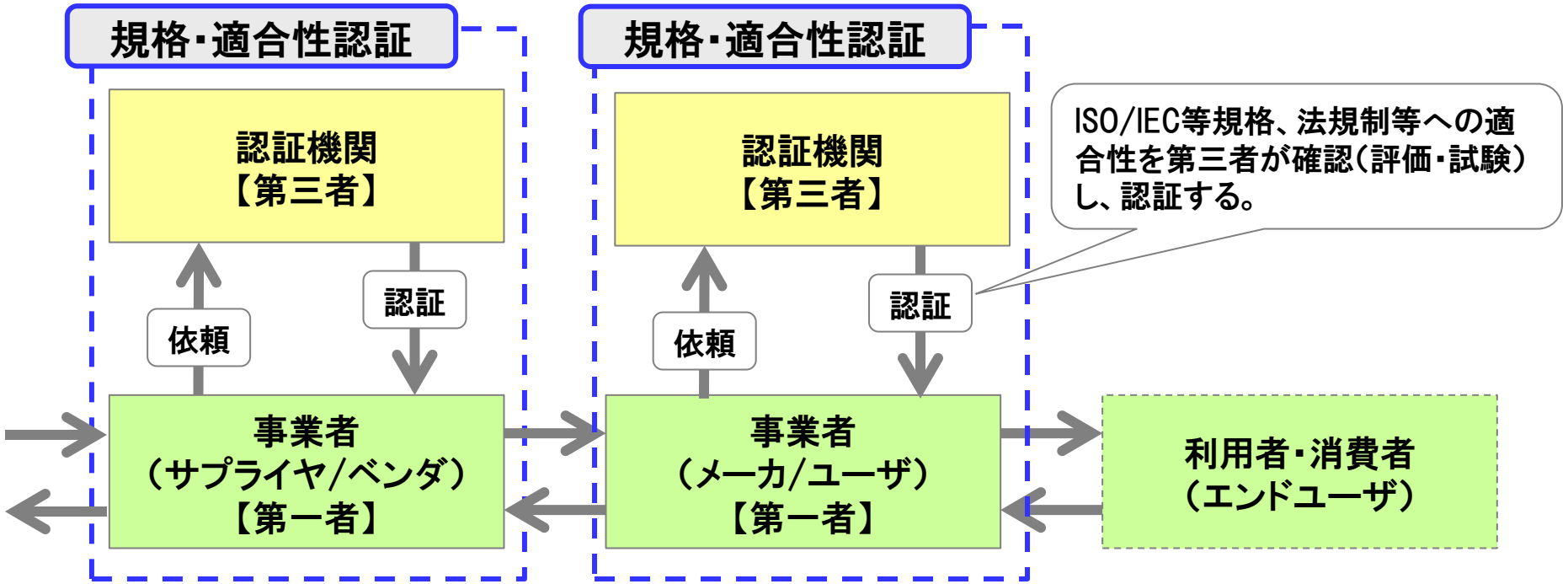
Copyright © 2012 IPA, All Rights Reserved

第三者による検証・妥当性確認の既存の枠組みとの関係
製品・サービスのサプライチェーン



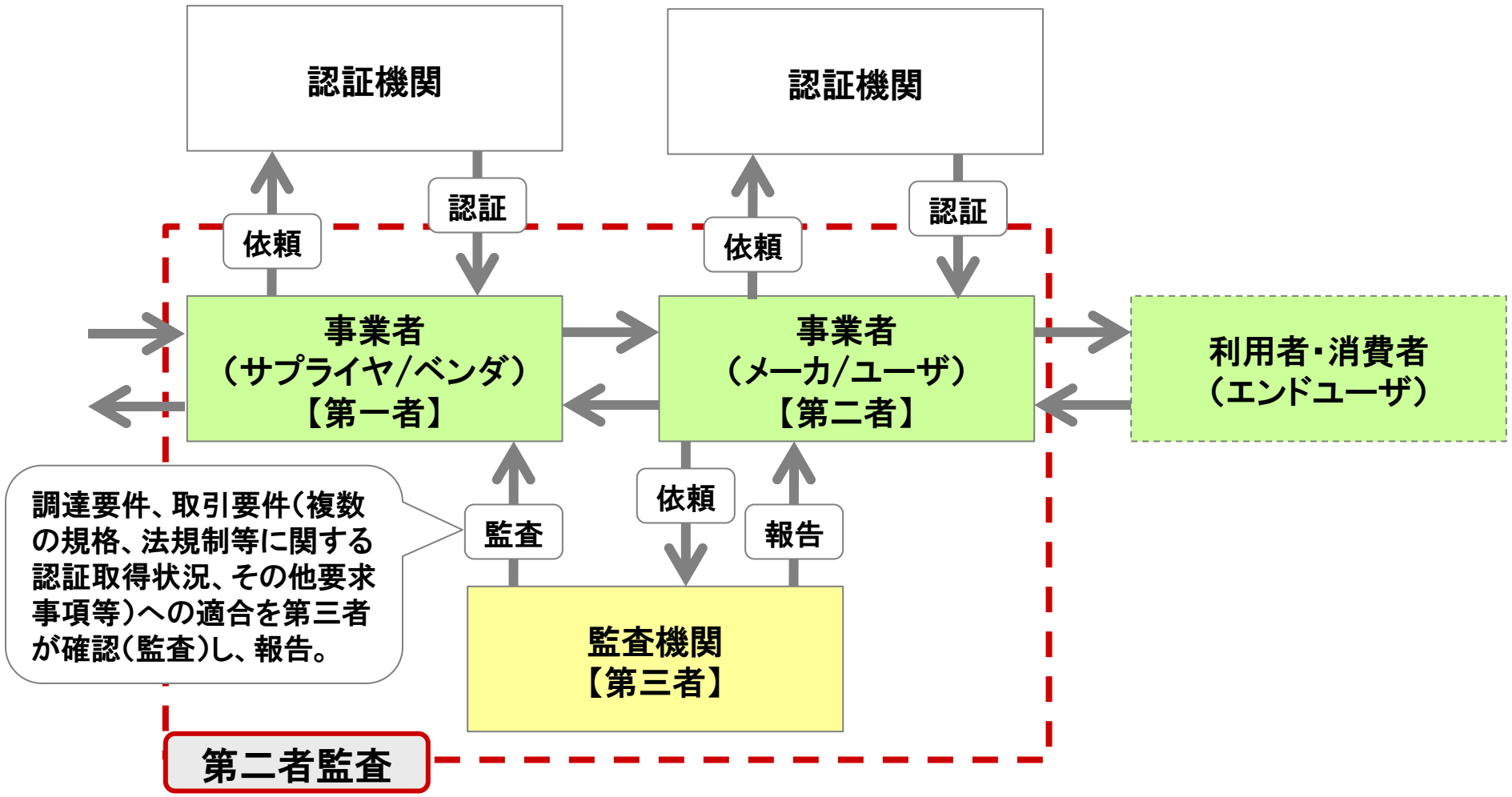
Copyright © 2012 IPA, All Rights Reserved

第三者による検証・妥当性確認の既存の枠組みとの関係
規格認証・適合性認証のフレームワーク



Copyright © 2012 IPA, All Rights Reserved

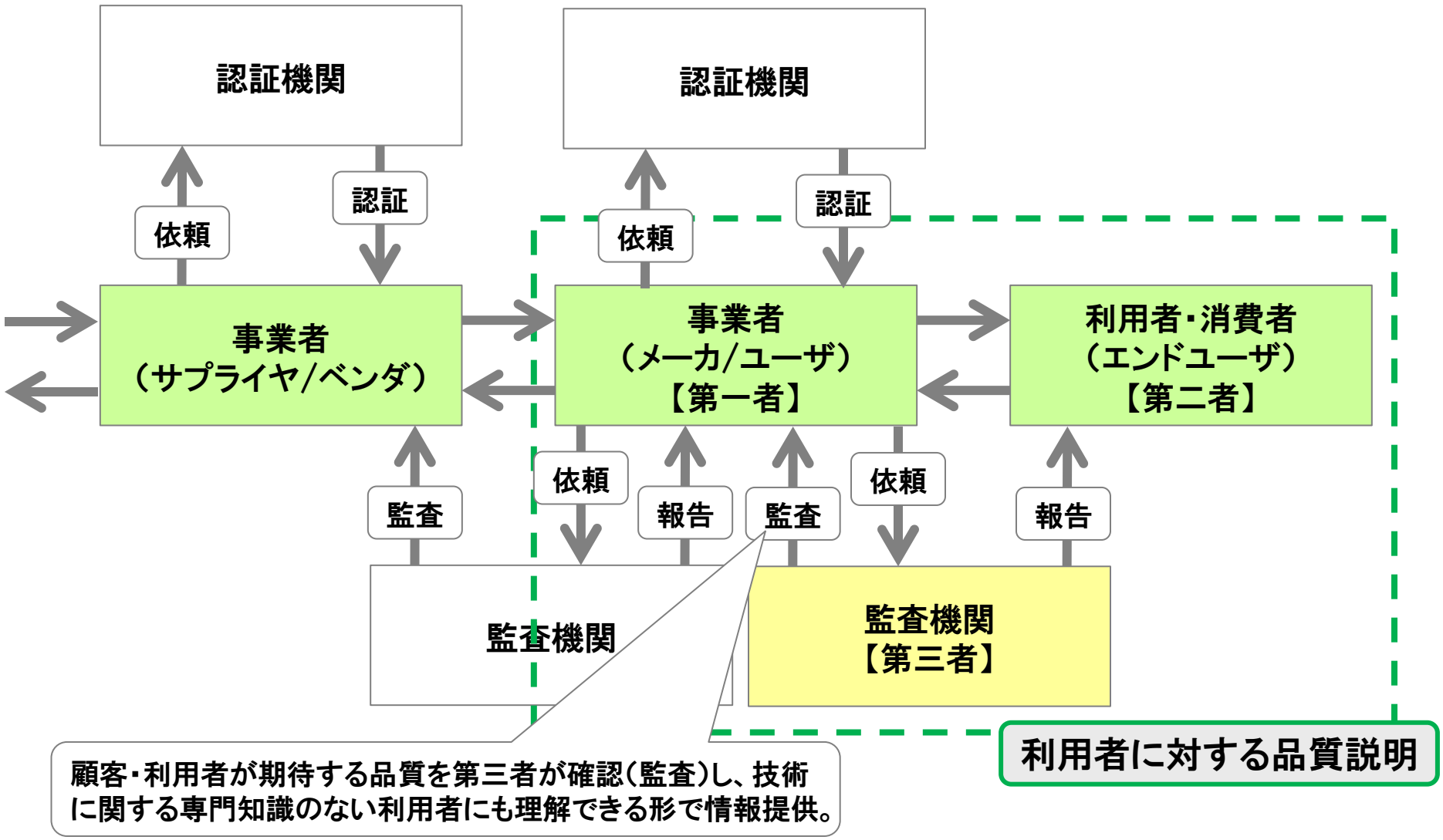
第三者による検証・妥当性確認の既存の枠組みとの関係
第二者監査のフレームワーク



Copyright © 2012 IPA, All Rights Reserved

第三者による検証・妥当性確認の既存の枠組みとの関係
利用者に対する品質説明力のためのフレームワーク

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri



Copyright © 2012 IPA, All Rights Reserved

ソフトウェア品質説明力強化のためのフレームワークの展開

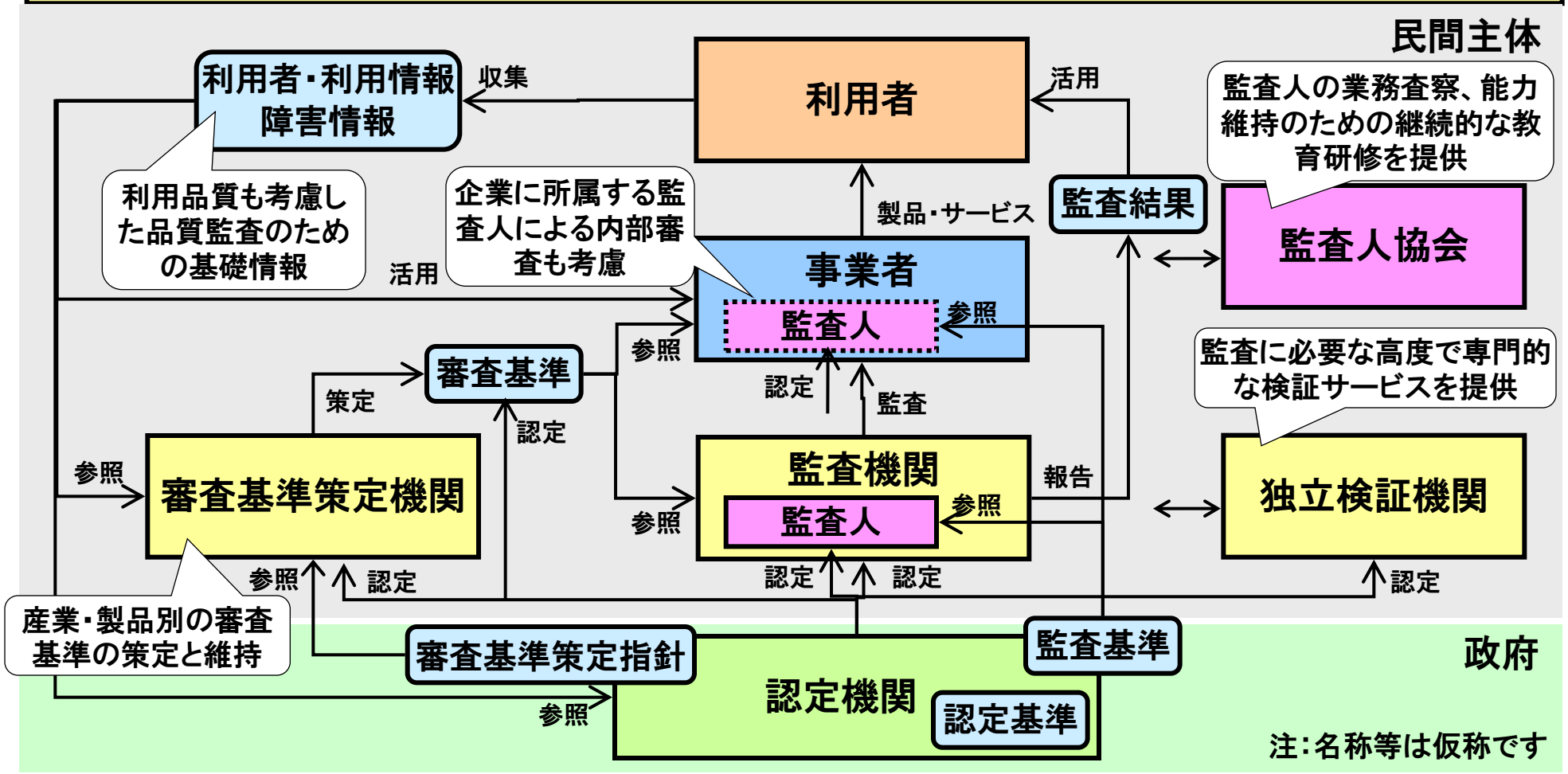
公的制度への展開：ソフトウェア品質監査制度（仮称）の枠組み

SEC
Software Engineering for Mo・No・Zu・Ku・Ri

下記の要件を満たす「監査人」が、産業分野あるいは製品分野毎に定められた「審査基準」を基に、「監査基準」に従って監査業務を遂行し、「監査結果」を利用者にも理解できる形で情報提供する制度

要件1．専門性：情報の信頼性を保証できる専門知識と能力を有していること

要件2．独立性：監査対象の事業者・利用者から身分的・経済的・精神的に独立していること



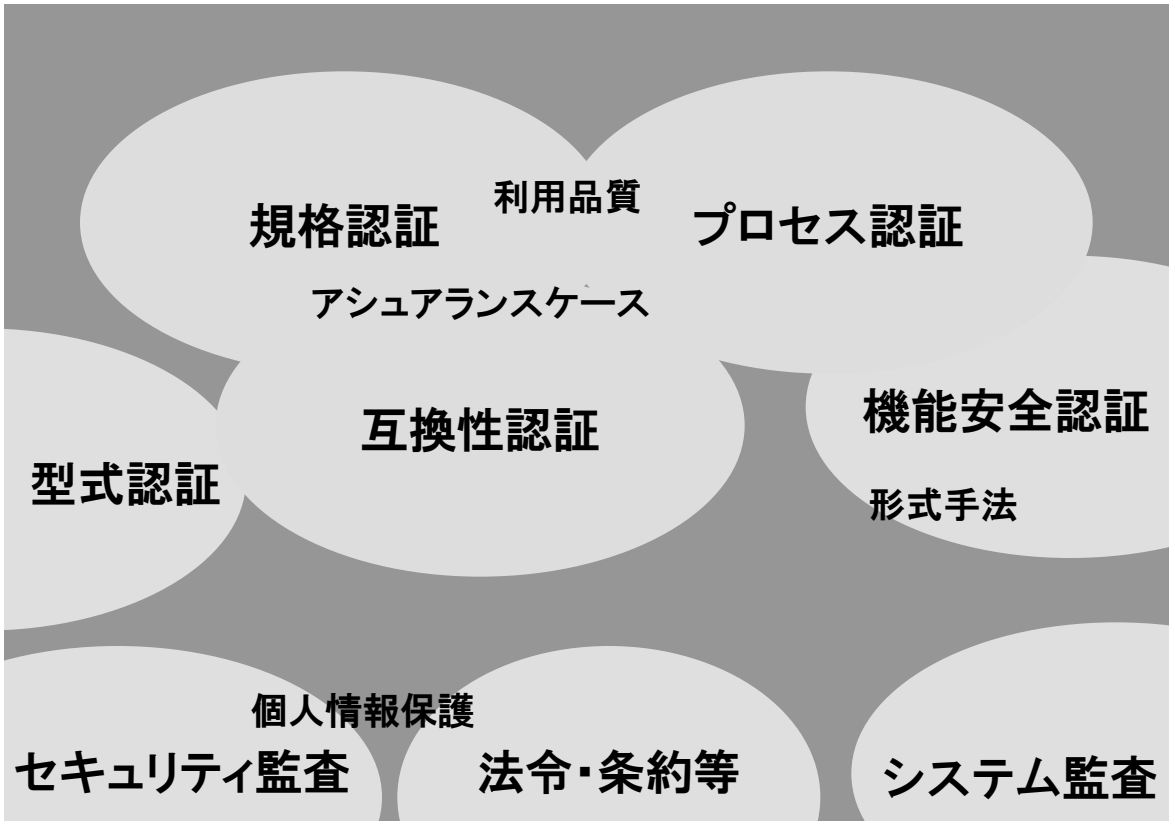
Copyright © 2012 IPA, All Rights Reserved

ソフトウェア品質説明力強化のためのフレームワークの展開
ソフトウェア品質監査制度（仮称）の特長

SEC
Software Engineering for Mo·No·Zu·Ku·Ri

- 独立検証機関による検証と妥当性確認を包含
  - 事業者の主張を高度な専門技術を持った独立検証機関で再確認
- 利用情報や利用者情報に基づく利用品質の確認
  - すべての開発ライフサイクルでの利用情報、利用者情報の活用を確認
- 既存の認証制度や監査制度を補完
  - 既存の認証結果・監査結果を確認し、重複した監査を簡略化
- 開発ライフサイクルに合わせて開発と並行して監査を実施
  - 指摘事項への対応による手戻りが防止でき、出荷時期等への影響を最小化
- 機密情報の拡散リスクを低減できる企業内部の監査人との連携
  - 監査人の管理下で企業内部の監査人が機密情報を直接アクセスする監査業務を実施

利用者・市場が期待する第三者による確認範囲



ソフトウェア品質監査制度（仮称）で監査する範囲
他の認証・監査の結果を確認する範囲

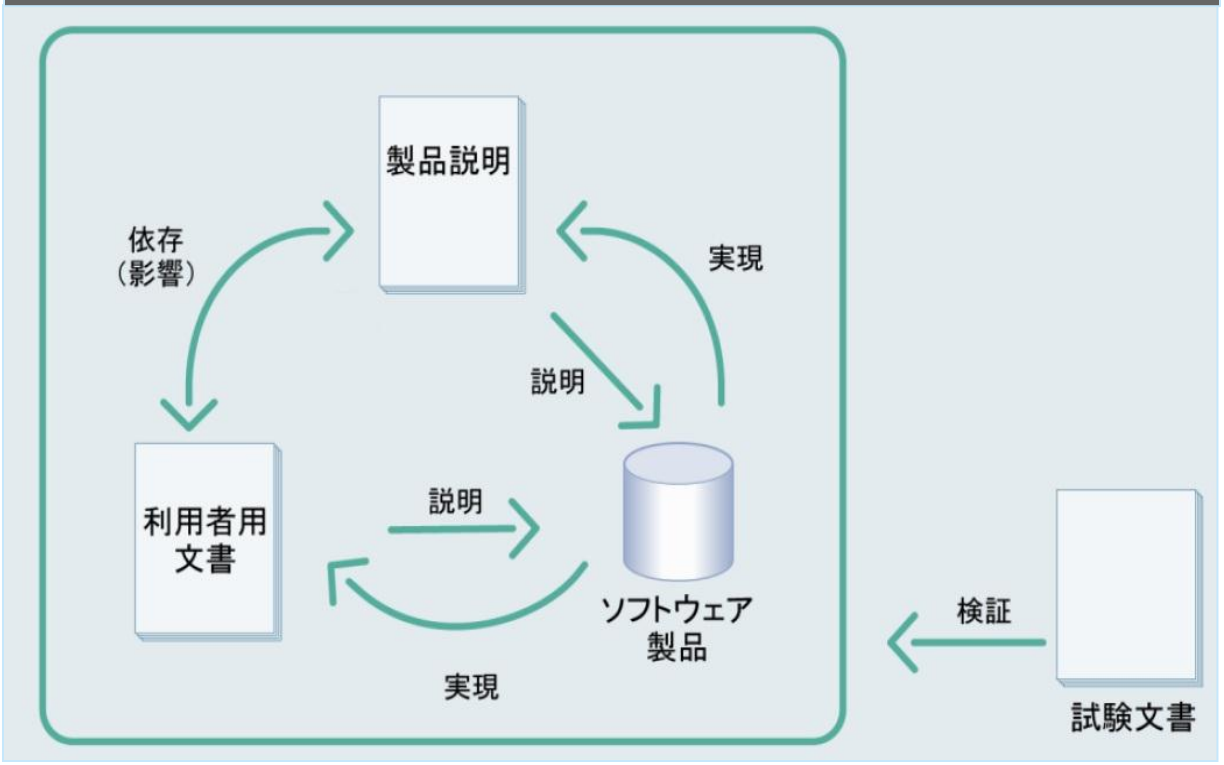
Copyright © 2012 IPA, All Rights Reserved

ソフトウェア品質説明力強化のためのフレームワークの展開
パッケージソフトウェア品質認証への展開：CSAJのPSQ認証の枠組み

- 一般社団法人コンピュータソフトウェア協会(CSAJ)が2013年度に創設を予定しているパッケージソフトウェア品質(PSQ)認証制度
- ソフトウェア製品の製品説明(カタログなど)、利用者用文書(マニュアルなど)がソフトウェア製品の機能と合致していることを第三者が確認し、CSAJが認証する制度

PSQ
Package Software
Quality Certification

PSQ認証制度が対象とする文書と製品の関係



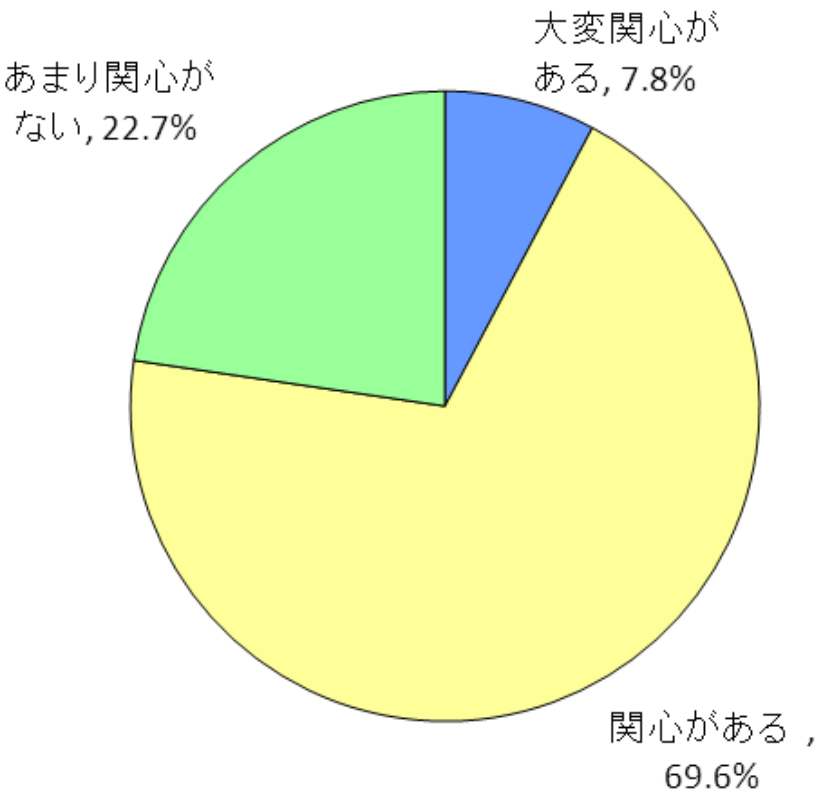
一般社団法人コンピュータソフトウェア協会の資料を元に作成

Copyright © 2012 IPA, All Rights Reserved

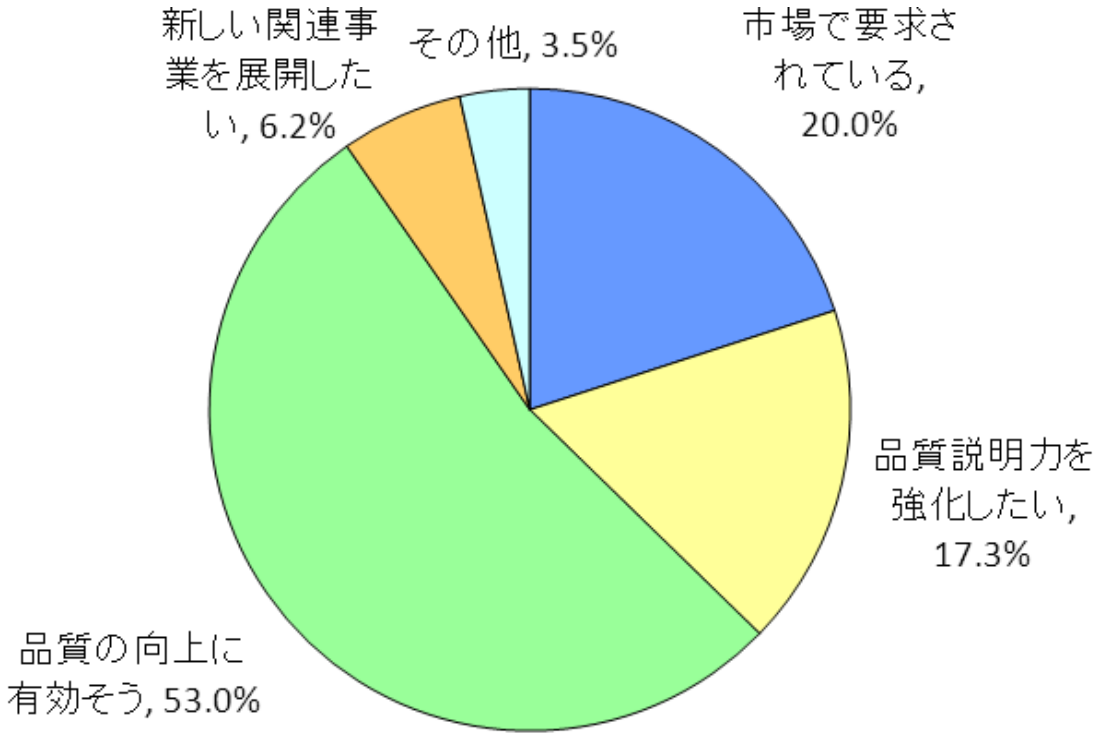
ESEC(2012年5月)のSECブース来場者のアンケート結果

SEC
Software Engineering
for Mo·No·Zu·Ku·Ri

品質監査制度(仮称)に関心がありますか？
(回答数:1508名)



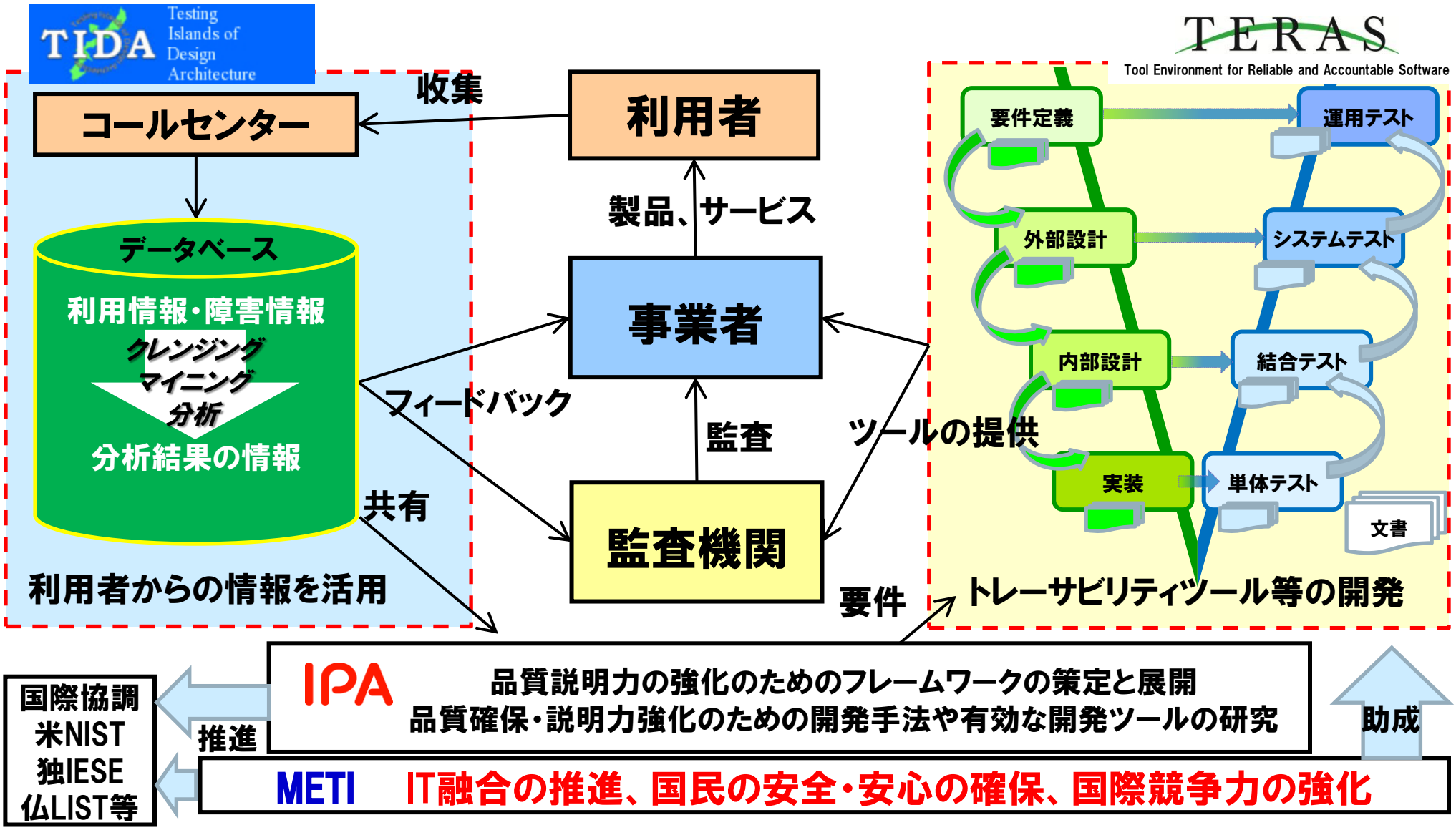
どのような観点で関心がありますか？
(回答数:1395名)



Copyright © 2012 IPA, All Rights Reserved
Copyright © 2012 IPA, All Rights Reserved

品質説明力強化に関連するプロジェクトとの連携

SEC
Software Engineering for Mo·No·Zu·Ku·Ri



Copyright © 2012 IPA, All Rights Reserved

一般社団法人TERASについて

TERAS：Tool Environment for Reliable and Accountable Software

- 設立　2011年4月7日
- 特別会員：　キャッツ㈱、豊通エレクトロニクス㈱、㈱電通国際情報サービス、
  日商エレクトロニクス㈱、㈱ベリサーブ、㈱エヌディーアイ、情報技術開発㈱
- 取組
  1. 日本の開発手法に適合したオープンなトレーサビリティ管理プラットフォームの開発
  2. 機能安全の国際規格への準拠活動
  3. 海外市場へ展開することでグローバルな開発環境構築支援
  4. 付加価値の高いソフトウェア業務への転換

TERASは、NTTデータグループ、豊通グループ、電通グループ、双日グループを含む14の企業・団体の参加*1)により2011年4月に設立された、産学官横断のプロジェクトです。
このプロジェクトでは、「トレーサビリティの向上」や「すり合わせ型開発」に有効な、オープンなツールプラットフォームの構築・提供を通じて、日本のソフトウェア産業基盤強化に貢献することを目的としています。

*1)　参加企業数は2011年8月現在

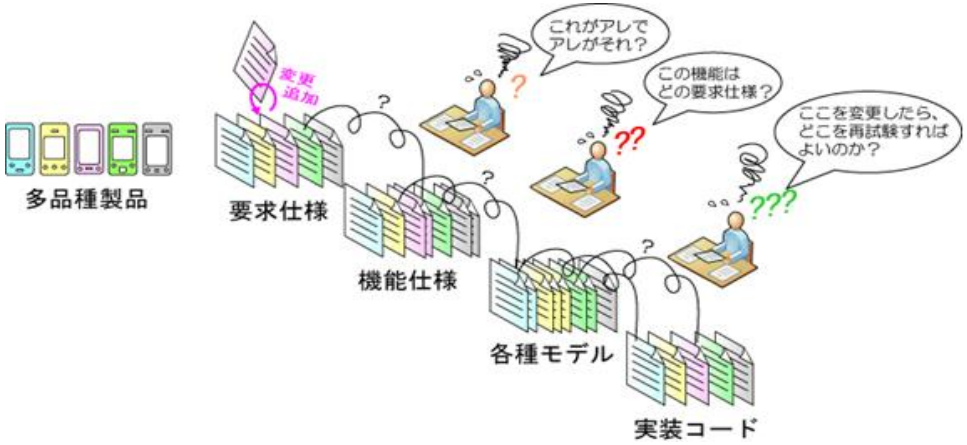
経済産業省　平成23年度産業技術実用化開発事業費補助金（組込みシステム基盤開発事業）の交付にて、開発費用の3分の2を国の助成により開発を行っていきます。

トレーサビリティとは？

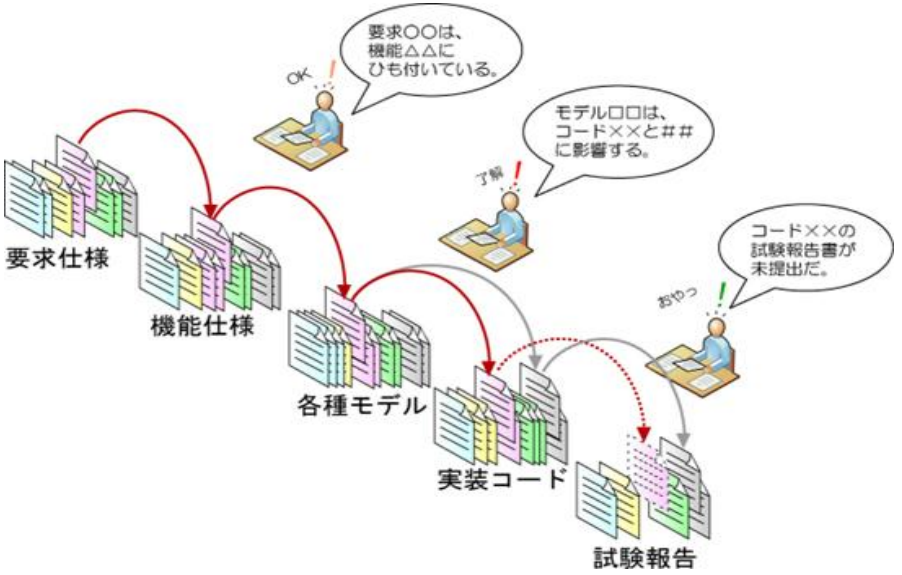
- システムの品質確保の手段である要求の管理が、重要になっています。
  - 要件がすべて設計、実装、試験されているか
  - 変更要求に対する修正モレはないか
  - 他の製品への影響はないか　　等々

これらを、関連する書類やプログラム、開発製品、関連部署、サプライチェーン企業群を含めた形で追っていける仕組みがトレーサビリティです。

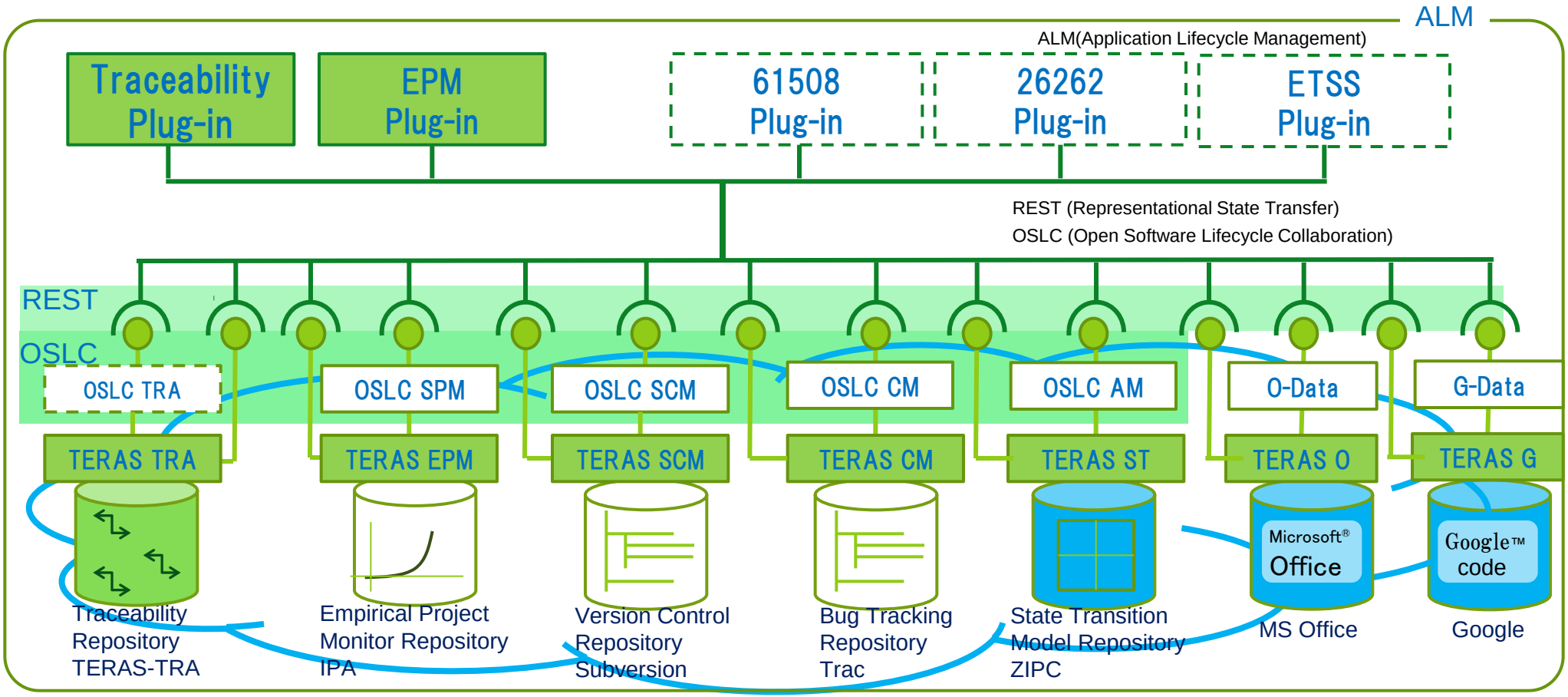
トレーサビリティなし



トレーサビリティあり



TERASプラットフォーム



TERAS提供予定　オープン提供　サードベンダー提供予定　オープン/サードベンダー提供予定

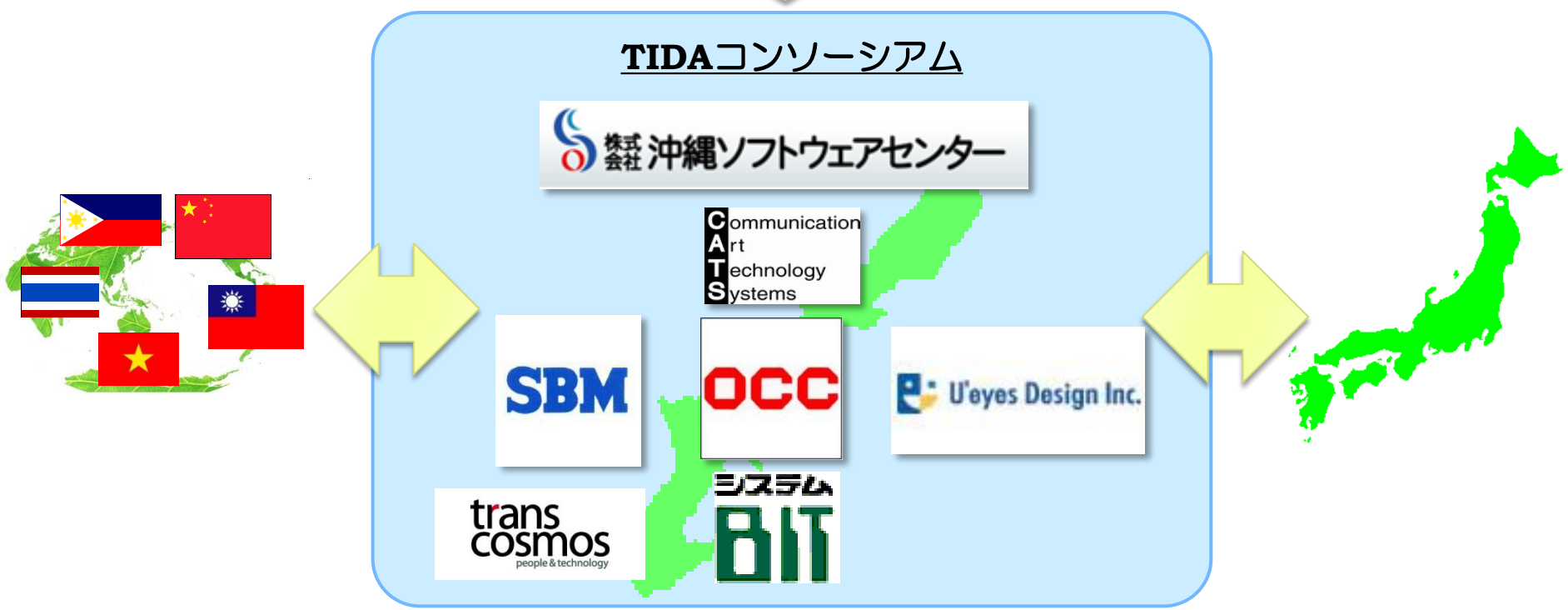
（技術委員会/WGでディスカッション中のシステム構成イメージ図）

ＴＩＤＡコンソーシアムについて

Testing Islands of Design Architectureの略称。沖縄県の補助のもと、製品のユーザ視点の信頼性と品質を向上させるための基盤技術（ツール）を構築することを目的とした沖縄県を中心として産官学横断のコンソーシアム。
2011年4月28日に設立。

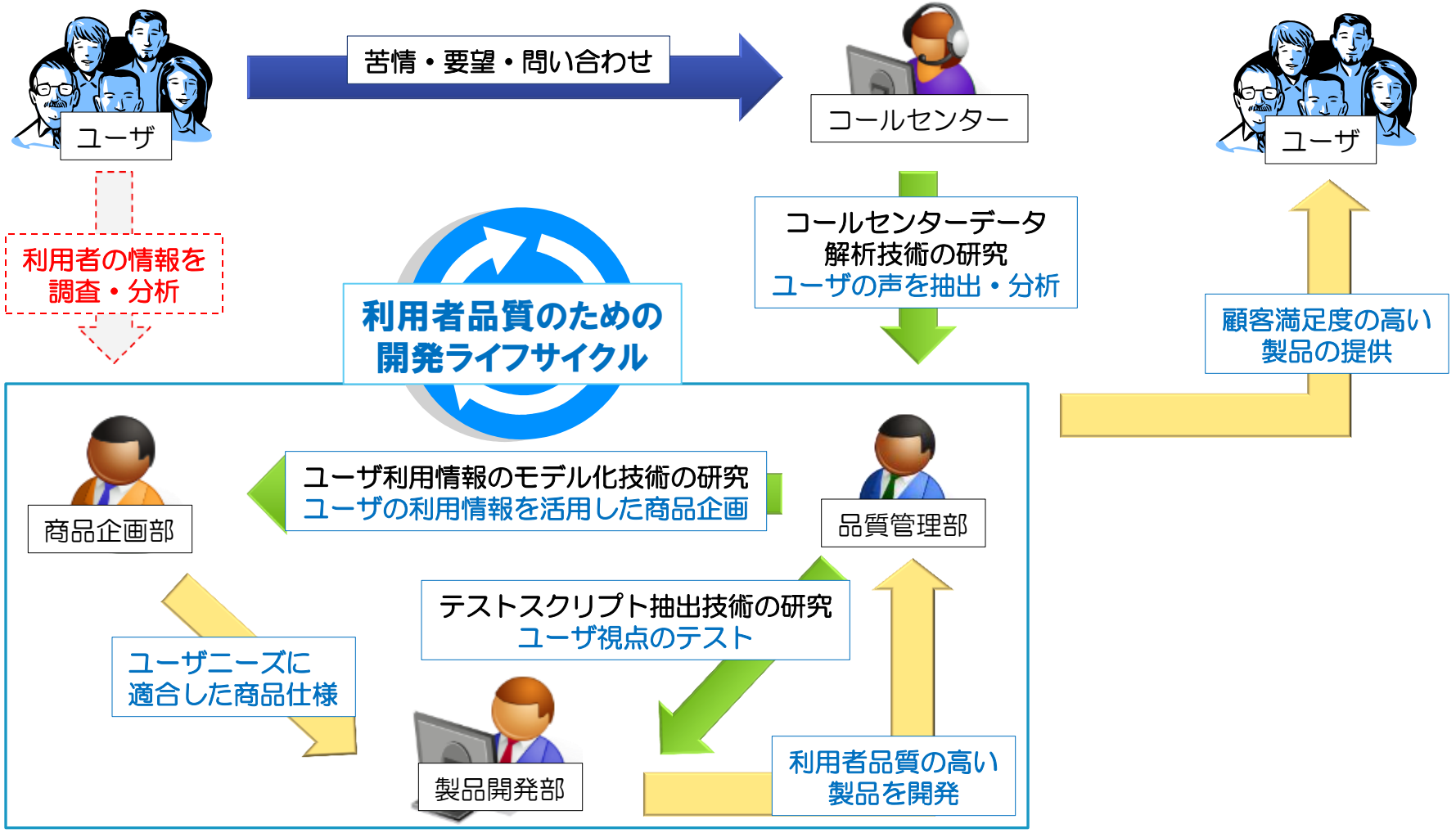
沖縄県

補助金（新たな組込みシステム検証基盤構築事業）

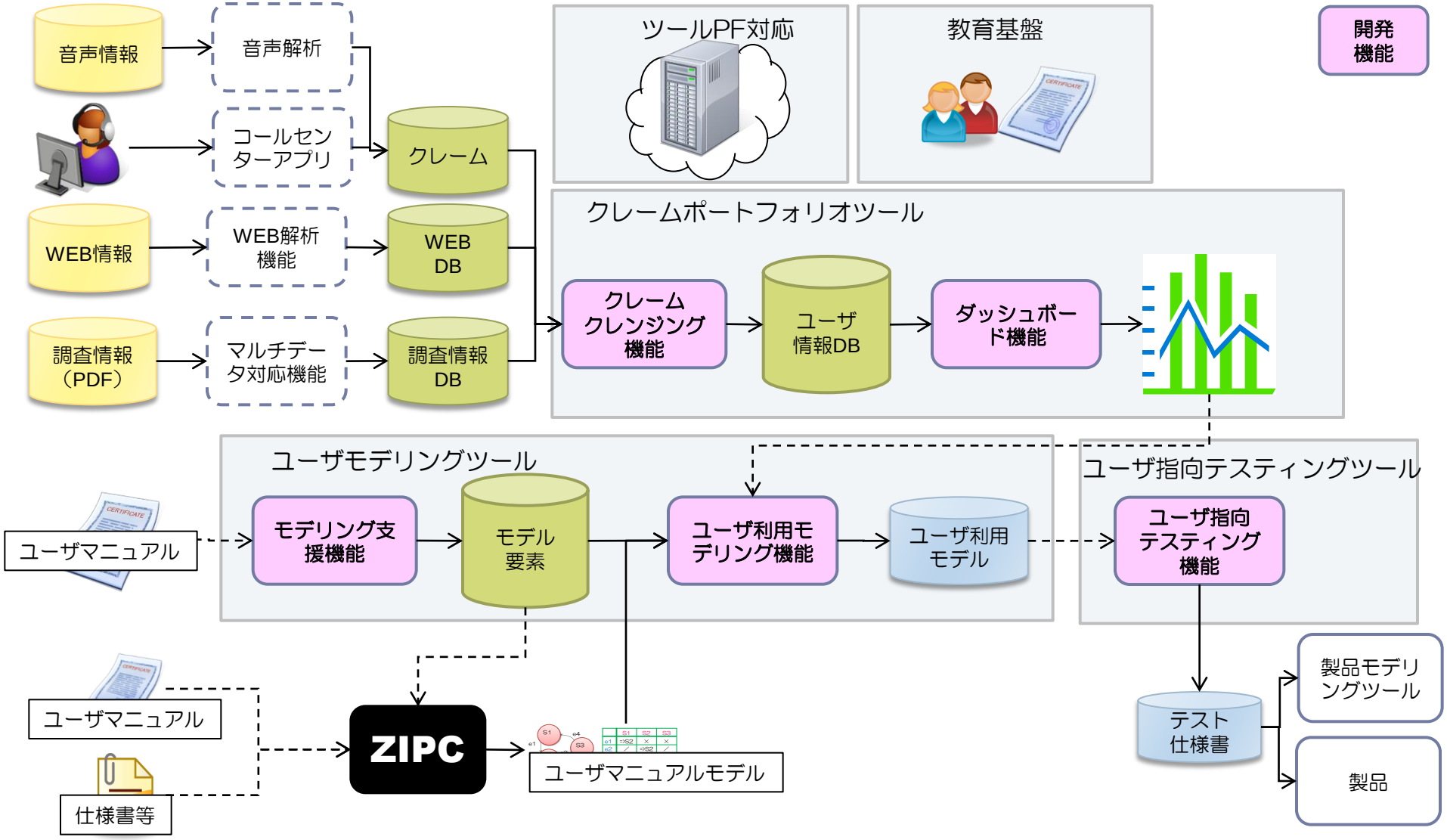


ＴＩＤＡコンソーシアムの目的

TIDAコンソーシアムの目的は、利用者品質を向上させるための開発ライフサイクルを支援する基盤技術（ツールなど）を構築することである。



TIDAコンソーシアムのツールチェーン



一般社団法人 スマートシステム検証技術協会

- 設立目的
  - 複数の企業から提供されるシステムが有機的に結合して構成されるスマートシステムの全体システムとしての信頼性、安全性などの利用者が求める品質を第三者が検証するための検証手法・検証技術を確立することにより、安全・安心・快適なスマート社会の実現に資することを目的とする。

- 実施事業
  - スマートシステムの検証手法・検証技術の確立のための事業
  - スマートシステムの検証手法・検証技術の普及・啓発のための事業
  - スマートシステムの検証手法・検証技術の応用に関する事業

- 設立日：2012年6月1日

- 住所　：大阪府淀川区西中島五丁目8番3号
  - WEB ：http://www.smartsystem.or.jp/

活動概要

- 目的:
  - 個々の機器をネットワークで接続して構成される
    スマートシステムの安全性を検証に必要な技術基盤の確立
    - このような基盤があれば、開発業者が提供する個々の機器のモデル等から
      スマートシステム全体の安全性を第三者が検証することが可能となる
- 目標:
  - スマートシステムの安全性検証フレームワークの確立

安全性検証フレームワーク

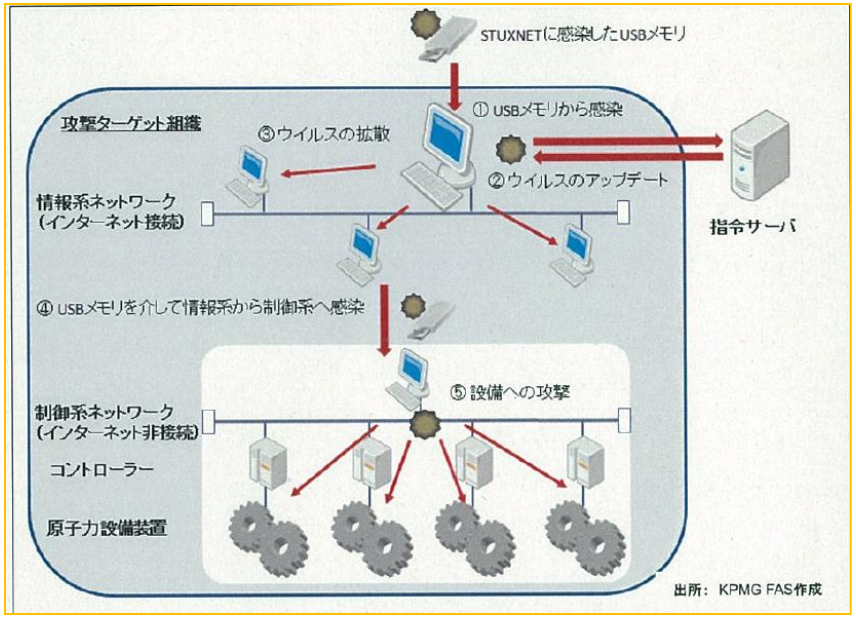
- リスク・ハザード分析手法
  - スマートシステムが安全であることを示すには、
    考えうる限りのリスクやハザードに対する対応が取られ、かつその対応が適切であることが必要
- スマートシステム全体のモデル記法
  - 個々の機器のモデルを接続
  - 分析されたリスクやハザードへの対応を盛り込む
- モデル上での検証技法
  - スマートシステムのモデルが求められる安全性を充足することを検証

リスク・ハザード分析手法

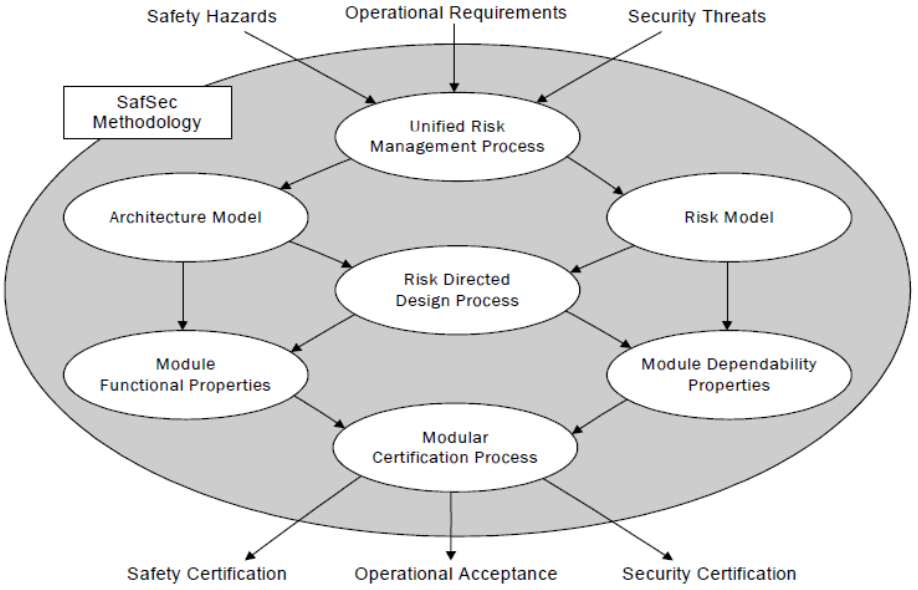
- 考えられる限りのリスクやハザードの分析を行い、その対応策を定める
  - 分析するリスクやハザードの例
    - システム特性の不整合
    - 機器の故障、設計不良
    - セキュリティ脅威
    - 誤操作等の人災
    - 落雷や地震等の天災

⇒ 分析結果をシステム全体の検証プロセス・検証項目に反映
（機能安全とセキュリティの一元化）

機器の故障モデルやセキュリティ脅威を含めての分析・対応が必須



Stuxnetによるイラン原子力設備の制御システムへの攻撃
⇒ 制御システムにもセキュリティ脅威が存在



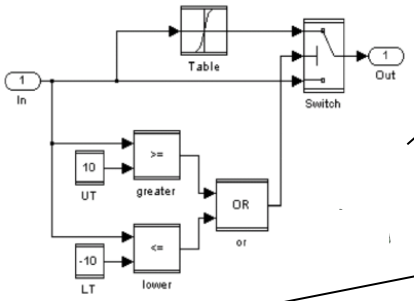
SafSec：セキュリティと安全性の同時認証方法論

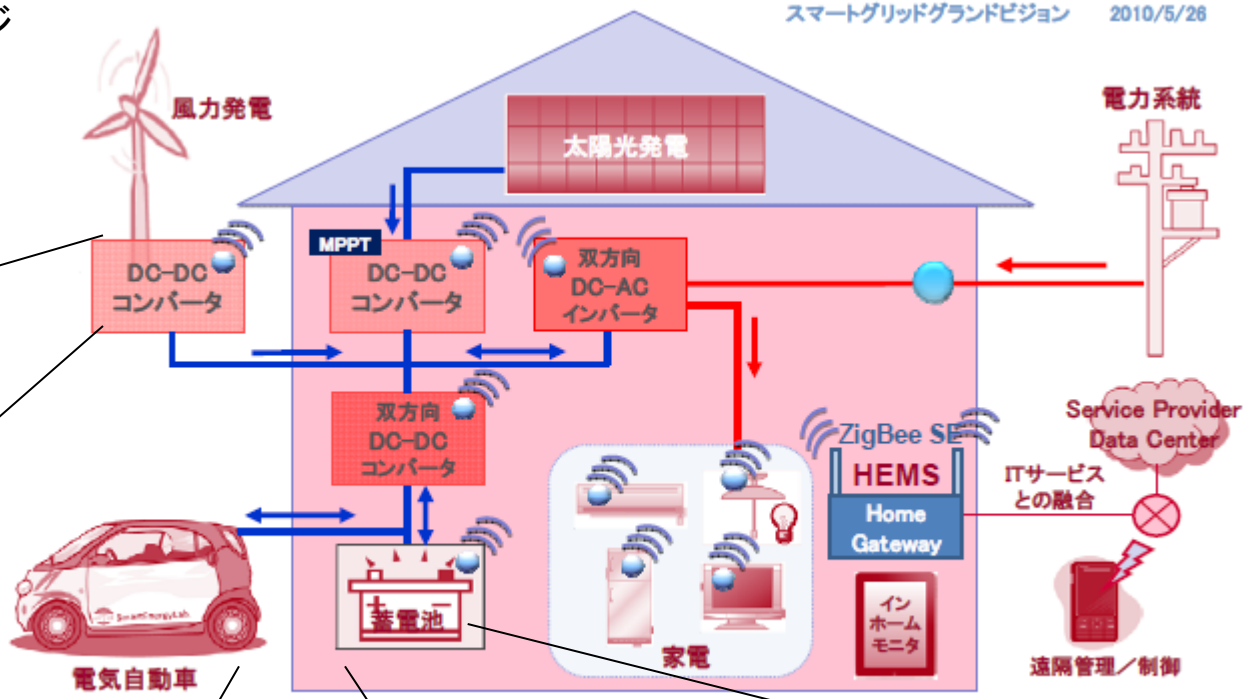
スマートシステム全体のモデル記述

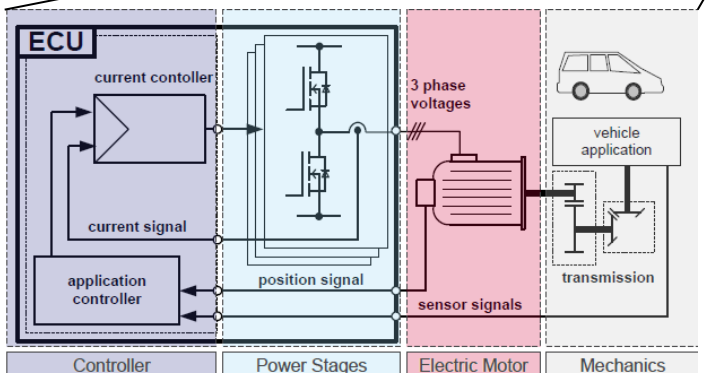
- 個々の機器の（連続/ハイブリッド）モデルを接続して全体のモデルを構成

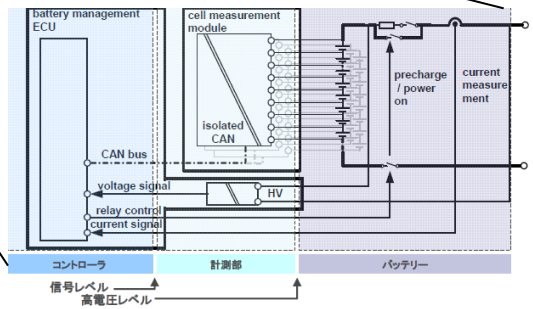
スマートハウス全体のモデルのイメージ
- バッテリの充放電
- バッテリの発熱
- 機器間の電流の流れ
- (バッテリ以外の)機器の電力消費
- バッテリマネジメントシステムの動作

等を接続



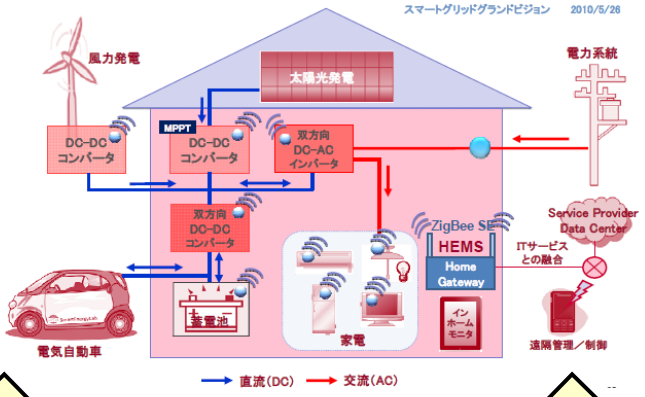






モデル上での検証技法

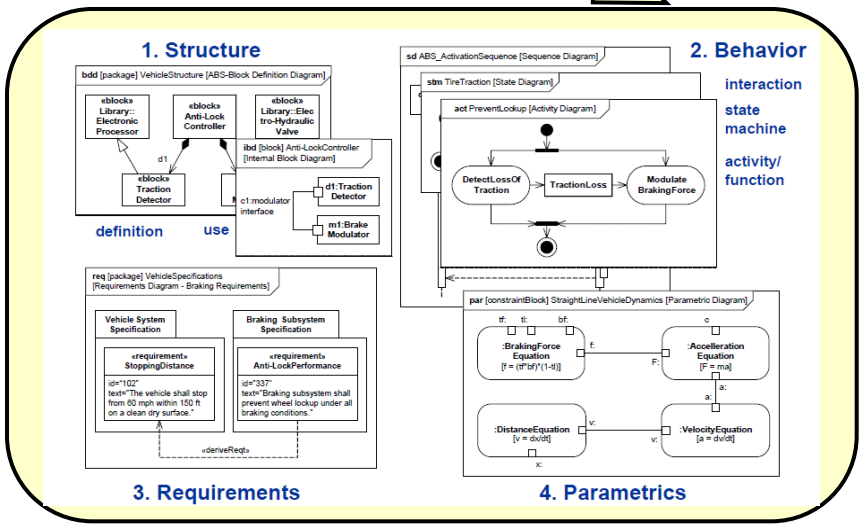
- 検証方法に応じた複数種類のモデル記述に基く総合的な検証手法を確立



想定されるあらゆる
リスクやハザードへの対応が
適切に取られていることを
適切な検証手法を選択しつつ、
システム全体の安全性が
満たされていることを検証

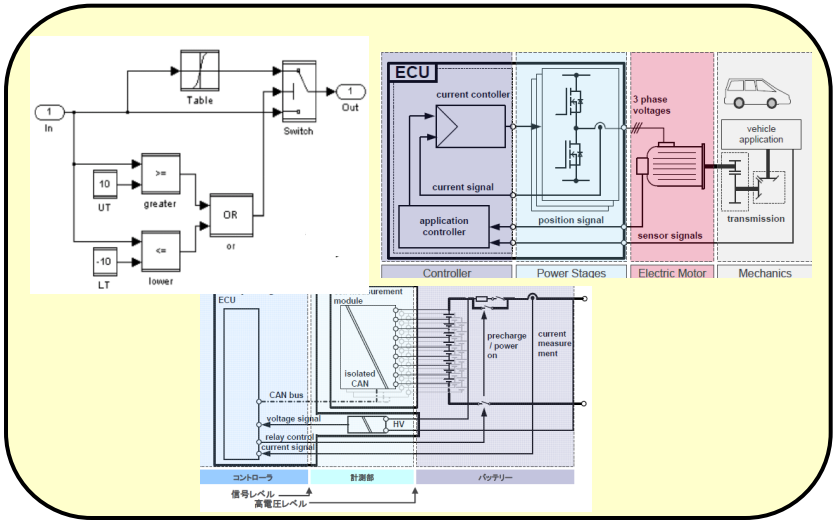
モデル全体の整合性
要求や数値制約の充足性
等の検証

シミュレーション



例えばSysML

互いに
変換可能



例えばMATLAB/Simulink

ご清聴ありがとうございました

Copyright © 2012 IPA, All Rights Reserved